DURIE TANGRI LLP
MARK A. LEMLEY (SBN 155830)
mlemley@durietangri.com
MICHAEL A. FELDMAN (SBN 295780)
mfeldman@durietangri.com
217 Leidesdorff Street
San Francisco, CA 94111
Telephone: 415-362-6666
Facsimile: 415-236-6300

AMY L. LANDERS (SBN 169491)
all328@drexel.edu
Professor of Law
Drexel University Thomas R. Kline School of Law
3200 Market Street
Philadelphia, PA 19104
Telephone: 215-571-4795

Attorneys for *Amicus Curiae*
Law Professors

IN THE UNITED STATES DISTRICT COURT

FOR THE 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.

Case No. CM 10-16-SP

~~[PROPOSED]~~ ORDER GRANTING MOTION OF NONPARTY LAW PROFESSORS FOR LEAVE TO FILE PROPOSED AMICUS CURIAE BRIEF

Date: March 22, 2016
Time: 1:00 p.m.
Ctrm: 3 or 4 - 3rd Floor
Judge: Honorable Sheri Pym

Having considered this matter and good cause appearing therefor,

IT IS HEREBY ORDERED that the pending Motion of Nonparty Law Professors for Leave to File *Amicus Curiae* Brief is hereby GRANTED.

SO ORDERED.

Dated: March 3, 2016

HONORABLE SHERI PYN
UNITED STATES DISTRICT JUDGE

PROOF OF SERVICE

I am a citizen of the United States and resident of the State of California. I am employed in San Francisco County, State of California, in the office of a member of the bar of this Court, at whose direction the service was made. I am over the age of eighteen years, and not a party to the within action. My business address is 217 Leidesdorff Street, San Francisco, CA 94111.

On March 3, 2016, I served the following documents in the manner described below:

PROPOSED] ORDER GRANTING MOTION OF NONPARTY LAW PROFESSORS FOR LEAVE TO FILE PROPOSED AMICUS CURIAE BRIEF

☐ (BY U.S. MAIL) I am personally and readily familiar with the business practice of Durie Tangri LLP for collection and processing of correspondence for mailing with the United States Postal Service, and I caused such envelope(s) with postage thereon fully prepaid to be placed in the United States Postal Service at San Francisco, California.

☐ (BY MESSENGER SERVICE) by consigning the document(s) to an authorized courier and/or process server for hand delivery on this date.

☐ (BY FACSIMILE) I am personally and readily familiar with the business practice of Durie Tangri LLP for collection and processing of document(s) to be transmitted by facsimile and I caused such document(s) on this date to be transmitted by facsimile to the offices of addressee(s) at the numbers listed below.

☐ (BY OVERNIGHT MAIL) I am personally and readily familiar with the business practice of Durie Tangri LLP for collection and processing of correspondence for overnight delivery, and I caused such document(s) described herein to be deposited for delivery to a facility regularly maintained by Federal Express for overnight delivery.

☒ BY ELECTRONIC SERVICE: By electronically mailing a true and correct copy through Durie Tangri's electronic mail system from mfeldman@durietangri.com to the email addresses set forth below.

☐ (BY PERSONAL DELIVERY) I caused such envelope to be delivered by hand to the offices of each addressee below.

On the following part(ies) in this action:

Eric David Vandevelde
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071
2132297186

Theodore J Boutrous, Jr.
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 900713197
2132297000

Fax: 2132296186
Email:
evandevelde@gibsondunn.com

Attorneys for Respondent Apple Inc.

Fax: 2132297520

Email: tboutrous@gibsondunn.com

Attorneys for Respondent Apple Inc.

Jeffrey G Landis
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
2022963585
Fax: 2027065298
Email: jeff@zwillgen.com

Attorneys for Respondent Apple Inc.

Theodore B Olson
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 200365306
2029558668
Fax: 2025309575
Email: tolson@gibsondunn.com

Attorneys for Respondent Apple Inc.

Nicola T Hanna
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 926124412
9494513800
Fax: 9494514220
Email: nhanna@gibsondunn.com

Attorneys for Respondent Apple Inc.

Marc J Zwillinger
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
2022963585
Fax: 2027065298
Email: marc@zwillgen.com

Attorneys for Respondent Apple Inc.

Allen W Chiu
AUSA Office
of US Attorney
National Security Section
312 North Spring Street Suite 1300
Los Angeles, CA 90012
2138942435
Fax: 2138946436
Email: allen.chiu@usdoj.gov

Attorneys for USA

Tracy L Wilkison
AUSA Office of US Attorney
Chief, Cyber and Intellectual Property
Crimes Section
312 North Spring Street 11th Floor
Los Angeles, CA 900124700
2138940622
Fax: 2138940141
Email: tracy.wilkison@usdoj.gov

Attorneys for USA

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on March 3, 2016, at San Francisco, California.

MICHAEL A. FELDMAN

DURIE TANGRI LLP
MARK A. LEMLEY (SBN 155830)
mlemley@durietangri.com
MICHAEL A. FELDMAN (SBN 295780)
mfeldman@durietangri.com
217 Leidesdorff Street
San Francisco, CA 94111
Telephone: 415-362-6666
Facsimile: 415-236-6300

AMY L. LANDERS (SBN 169491)
all328@drexel.edu
Professor of Law
Drexel University Thomas R. Kline School of Law
3200 Market Street
Philadelphia, PA 19104
Telephone: 215-571-4795

Attorneys for *Amicus Curiae*
Law Professors

IN THE UNITED STATES DISTRICT COURT

FOR THE 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.	Case No. 5:16-cm-00010-SP ***AMICUS CURIAE* BRIEF OF LAW PROFESSORS IN SUPPORT OF APPLE, INC.** Date: March 22, 2016 Time: 1:00 p.m. Ctrm: 3 or 4 - 3rd Floor Judge: Honorable Sheri Pym

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES (Cont'd)

Page(s)

TABLE OF AUTHORITIES (Cont'd)

Page(s)

Statutes

Other Authorities

TABLE OF AUTHORITIES (Cont'd)

Page(s)

Rules

INTEREST OF AMICI

Amici are law professors at schools throughout the United States. We have no personal interest in the outcome of this case, but a professional interest in seeing that the law develops to encourage creativity and innovation, and to advance the public interest. No one other than the undersigned wrote or funded any portion of this brief. Institutional affiliations are given for identification purposes only.

I. INTRODUCTION

The government has gone to great lengths to sidestep due process in its effort to avoid judicial scrutiny of the merits of its case. And for good reason: its case lacks merit.

The Department of Justice and the FBI demand that Apple dedicate its employees and hundreds of hours of employee time to develop software that provides a way to break into iPhones. That software does not currently exist. In fact, Apple specifically chose not to create it in the course of its business. The government now claims it can conscript Apple to create software Apple does not want to create and then force Apple to assist the government in using that software. The record demonstrates that government access requests will not stop with this single device.[1]

Although the government admits it had the time to—and, in fact, did—first approach Apple informally instead of going directly to the courts, and although the government presents no plausible reason for needing an immediate answer now, the DOJ and FBI filed their demand *ex parte*, depriving this Court of the benefit of Apple's perspective. Moreover the government acknowledges that the motion to compel was not

[1] Declaration of Nicolat Hanna in Support of Apple Inc.'s Motion to Vacate Order Compelling Apple, Inc. to Assist Agents in Search and Opposition to Government's Motion To Compel Assistance ("Hanna Decl.") ¶ 5 & Ex. C, *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*, No. 5:16-cm-00010-SP ("Case No. 16-10") (C.D. Cal. Feb. 25, 2016), ECF Nos. 16-1 & 16-4.

necessary.[2]

The government's actions cloud the legal and factual landscape. Once the fog lifts, it is clear that multiple laws, constitutional provisions, and judicial doctrines prohibit precisely what the government demands. Compelling a private company to create technology with features that the firm deliberately chose to exclude is an unprecedented expansion of judicial power that Congress did not support by passing the All Writs Act.

First, there is a jurisdictional problem. There is no basis in the record for this Court to assert Article III jurisdiction to issue or enforce the February 16, 2016 Order ("the Apple Order"). The search warrant's authority is already exhausted and the government's motion to compel recognizes that CALEA ("Communications Assistance for Law Enforcement Act") does not provide sufficient authority to support the Apple Order. Rather, the government's request rests solely on the All Writs Act. However, the All Writs Act is not an original source of federal jurisdiction and cannot support the government's motion or this Court's order. The All Writs Act merely provides a source of residual authority *where such jurisdiction independently exists*.

Second, the underlying Order is invalid because it deprives Apple of liberty and property without due process of law. The government initially took the time to seek Apple's help outside the judicial process. Only after Apple declined did the government file its *ex parte* application, which did not allow Apple an opportunity to respond. Even though Apple has now had an opportunity to respond to the government's motion to compel, the underlying Apple Order itself was issued in violation of due process and must be vacated.

///

---

[2] The government acknowledges that "a separate order compelling Apple's compliance with this Court's February 16, 2016, order is not legally necessary . . . ," suggesting that it filed "this noticed motion to provide Apple with the due process and adversarial testing it seeks." Case No. 16-10 (C.D. Cal. Feb. 19, 2016), ECF No. 1 (Gov't's Mot. to Compel Apple Inc. to Comply with This Court's Feb. 16, 2016 Order Compelling Assistance in Search) at 3 n.3. However, as discussed below, Apple must be afforded the opportunity to challenge the merits of the Apple Order itself, not merely the motion to compel.

Third, CALEA and ECPA ("Electronic Communications Privacy Act") govern the substantive validity of the Order and set out telecommunications carriers' obligations to assist law enforcement. Significantly, when Congress enacted CALEA, it exempted "information services," which includes certain services that Apple provides, from that requirement. The Supreme Court has instructed that where a statutory scheme governs a particular subject matter, the All Writs Act's residual power does not.

Finally, no court has ever issued a valid order that imposes an equivalent burden on a non-party. Our research has not found *any* case that uses the All Writs Act to require a third-party private entity to design and create new software. Some courts have compelled disclosure of already-existing information in cases where the All Writs Act is found applicable. In contrast, the order the government demands in this case would require substantial expenditures of time and talent above and beyond what is appropriate under the All Writs Act. This point is particularly alarming where Apple has made a deliberate decision to *exclude* the features that the government now demands.

The issues in this case—particularly those concerning the All Writs Act—raise important concerns for privacy interests globally and the security of the technical infrastructure on which many in this country depend. The order the government demands here threatens to give the government *de facto* control over the course of technical innovation, favoring police access to evidence over the security of our technical infrastructure as well as individual privacy.

II. THIS COURT LACKS JURISDICTION TO ISSUE AND ENFORCE THE APPLE ORDER

The government is proceeding in this Court on the basis of a search warrant that Magistrate Judge David Bristow issued on December 3, 2015. *See* Declaration of Christopher Pluhar ¶ 5 & Ex. 1, *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*, No. 15-0451-M ("Case No. 15-451") (C.D. Cal. Feb. 16, 2016), ECF No. 16. The search warrant allows law enforcement to search a Black Lexus IS300 and to

seize certain items, including "digital device[s]" and evidence about those digital devices. The FBI searched the car and found the iPhone that is at issue here. The government now has that phone and may search it consistent with the limitations imposed by the December 3, 2015 warrant. With that, the warrant's authority is exhausted.

The government concedes that neither CALEA nor Federal Rule of Criminal Procedure 41 provides authority to require Apple to create software to access data now stored on the device. *See* Case No. 16-10, ECF No. 1 at 22. Instead, the government's request rests solely on the All Writs Act. *Id.* However, the All Writs Act cannot support the government's motion or this Court's order.

The All Writs Act provides a source of residual authority to federal courts "in aid of their respective jurisdictions" *where such jurisdiction independently exists. See* 28 U.S.C. § 1651(a). A court must have Article III jurisdiction before it can issue an extraordinary writ. 16B Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 4005 (3d ed. 2015). By itself, the All Writs Act is incapable of serving as an original source of federal jurisdiction. *See Syngenta Crop Prot. v. Henson*, 537 U.S. 28, 33 (2002). Therefore, this district court lacks jurisdiction to issue and enforce the Apple Order. *See In re U.S. For an Order Directing a Provider of Commc'n Servs. to Provide Tech. Assistance to Agents of the U.S. Drug Enf't Admin.*, --- F. Supp. 3d ---, No. 15-1242 (M), 2015 WL 5233551, at *5 (D.P.R. Aug. 27, 2015). Because this Court lacks Article III jurisdiction to issue or enforce the Apple Order, it should vacate the order.

III. NEITHER THE DEPARTMENT OF JUSTICE NOR THE COURTS HAVE YET AFFORDED APPLE DUE PROCESS OF LAW

The right to be heard is fundamental to due process of law in an adversary system in both criminal and civil contexts. *See Clemons v. Mississippi*, 494 U.S. 738, 769 (1990) (quoting *Rock v. Arkansas*, 483 U.S. 44, 51 & n.9 (1987)); *Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). The adversary system relies on the opportunity for both sides to offer their perspectives so that the Court may have a full understanding before it issues a ruling. Yet the government filed its All Writs Act

application *ex parte*, requiring this Court to make a decision based on a skewed and incomplete understanding of the facts and legal landscape. Due process requires more.

The Fifth Amendment is clear that "No person shall be . . . deprived of life, liberty, or property, without due process of law." Courts have consistently applied Fifth Amendment due process protections to the All Writs Act, including similar cases involving Apple. *See, e.g.*, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, No. 1:15-mc-01902-JO, 2015 WL 5920207, at *7 (E.D.N.Y. Oct. 9, 2015) ("[C]ourts have held that due process requires that a third party subject to an order under the All Writs Act be afforded a hearing on the issue of burdensomeness ***prior to*** compelling it to provide assistance to the Government.") (quoting *In re XXX, Inc.*, No. 14 Mag. 2258, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014)) (emphasis added). In this case, the government seeks to deprive Apple of both property[3] and liberty.[4] To determine whether due process was adequate to support this deprivation, courts consider three factors: (1) the importance of the individual's interest at stake, (2) the likelihood that more formalized procedures would avoid arbitrary or erroneous decisions by the government, and (3) the countervailing government interest (such as the efficiency of government administrative agencies. *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976). In this case, each of these factors weighs *against* the government's demand.

---

[3] The government demands that Apple develop new software that would be protected both as a trade secret, *see Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) (finding that trade secrets are property rights subject to constitutional protections, such as the takings clause), and as copyrighted software, *see* 3 Patry on Copyright § 9:240 n.2 ("Computer programs are, of course, generally classified as 'literary works' [under the Copyright Act].").

[4] Apple has a liberty interest in operating its company as it chooses to. *Cf. Greene v. McElroy*, 360 U.S. 474, 492 (1959) (finding that "the right to hold specific private employment and to follow a chosen profession free from unreasonable governmental interference" is a liberty interest protected by the Due Process Clause); *Bd. of Regents of State Colls. v. Roth*, 408 U.S. 564, 572 (1972) (holding that liberty "denotes not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, [and] to acquire useful knowledge" among other rights).

A. Apple's Interests at Stake in this Case are Critical

Apple has made a conscious decision as part of the operation of its business to build in an iPhone Unique ID that is necessary to decrypt the data on the phone and which Apple itself does not know. *See* Case No. 16-10 (C.D. Cal. Feb. 25, 2016), ECF No. 16 (Apple's Mot. To Vacate) at 5–7, 23. The government's demand would interfere with a private company's decisions about which software and security it will develop and which it will not. Apple's business is developing technology—both physical and intellectual property. Whether the government can dictate the technology Apple must develop and force Apple to turn that technology over to the government is a vitally important interest.

B. A More Formalized Procedure to Consider Apple's Perspective is Likely to Avoid Arbitrary or Erroneous Decisions

This Court, and courts addressing similar issues in the future, are likely to reach arbitrary or erroneous decisions without a formalized process for Apple—or another future company—to be heard. Because this Court issued its February 16, 2016 order without the benefit of a hearing or briefing from Apple, it made its decision on incomplete and misleading information.

For instance, the government represented in its *ex parte* application that it was not asking to place an "unreasonable burden" on Apple because "while the order . . . requires Apple to provide modified software . . . it is not an unreasonable burden for a company that writes software code as part of its regular business." *See* Case No. 15-451 (C.D. Cal. Feb. 16, 2016), ECF No. 18 at 14–16. This proves too much. By this same logic, it would not be unreasonably burdensome to demand that Boeing build a custom jet for the government because Boeing builds planes as part of its regular business or to demand that a pharmaceutical company make drugs for executions after it has made the intentional decision not to. With the benefit of Apple's briefing, the Court can consider Apple's perspective on the burden of developing, testing, implementing, and protecting custom code for this investigation. *See* Case No. 16-10, ECF No. 16 at 23–30.

///

Apple's perspective is also critical to the security of consumers using Apple devices. The government demanded that this Court order Apple to develop software without allowing Apple the opportunity to explain the risks involved in the way the government wants Apple to develop its software. Allowing the government to dictate how Apple develops software can create very real privacy and security risks for Apple users. Computer scientists have shown that grave risks arise from requiring the introduction of insecure software. *See* H. Abelson et al., *Keys under doormats: mandating insecurity by requiring government access to all data and communications*, J. of Cybersecurity, 69–79 (2015). Apple is better suited than the government to address potential privacy and security problems in development of its own software. It is therefore critical that Apple have the opportunity to address these considerations to the Court *before* it issues an order.

The government also represented that new Apple software is "necessary" to collect data from the iPhone. *See* Case No. 15-451, ECF No. 18 at 16–17. However, with the benefit of Apple's briefing, the Court learned that the FBI *created* this situation. Case No. 16-10, ECF No. 16 at 11. As Apple explains in its motion to vacate, the iPhone might have been able to initiate an automatic iCloud backup, allowing the FBI access to the information it wants. *See id.* at 29–30. However, the FBI changed the iCloud password on the account associated with the iPhone without consulting Apple, making it impossible to trigger the automatic backup. *See id.*

Finally, the government's application for the Apple Order makes no mention of CALEA or ECPA despite the fact that these statues govern this precise issue: the scope of responsibilities for a third party to provide assistance to law enforcement in obtaining electronic communications evidence. Without Apple's brief, the Court did not have the opportunity to consider the limitations of CALEA, which "does not authorize any law enforcement agency or officer . . . to require any specific design of equipment, facilities, services, features . . . ." 47 U.S.C. § 1002(b)(1)(A). CALEA is directly relevant to the question whether the order the government demands is "agreeable to the usages and

principles of law." 28 U.S.C. § 1651(a).

These facts and legal background are vital to a Court's reasoned decision. Without them, the Court risks arbitrary or erroneous decisions.

C. The Government Has No Substantial Countervailing Interest in Expediency

The government cannot show any compelling interest in expediency. *Ex parte* proceedings were not necessary because the government had time to ask Apple to assist voluntarily, as the government itself admits. *See* Case No. 15-451, ECF No. 18 at 16–17. If the government had time to ask Apple to assist voluntarily before demanding Court intervention, the Court had time to consider Apple's position *before* issuing its order.

* * *

The government's *ex parte* motion and this Court's order deprived Apple of its liberty and property without due process of law. Apple was entitled to a hearing and opportunity to be heard *before* this Court issued an order conscripting its services in support of law enforcement. It is not enough that Apple now has the opportunity to challenge the government's motion to compel. The Apple Order itself issued without affording Apple an opportunity to be heard and therefore suffers from the errors and arbitrariness discussed above in Section III(B). Even if the Court denies the government's motion to compel, the Apple Order would still stand and might be considered precedential. Thus, the Court should vacate the underlying Apple Order because it issued in violation of due process.

IV. THE FIRST CONGRESS INTENDED THE ALL WRITS ACT TO BE MORE LIMITED THAN THE GOVERNMENT NOW SUGGESTS

The All Writs Act, 28 U.S.C. § 1651 (a), provides that the federal courts "may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." The All Writs Act derives from the Judiciary Act of 1789, enacted by the country's first Congress in order to create the federal court system.

///

The context of this enactment is critical to understanding the present dispute. Congress tasked the federal courts with a significant role that was, nonetheless, constrained. *See* Paul Taylor, *Congress's Power to Regulate the Federal Judiciary: What the First Congress and the First Federal Courts Can Teach Today's Congress and Courts*, 37 Pepp. L. Rev. 847, 857 (2010). When the first Judiciary Act was promulgated, state courts already existed. Yet the Federal system was found to be necessary to, among other things, protect the population's liberty interests "from hasty or undue encroachment by the federal government." William N. Eskridge, Jr., *All About Words: Early Understandings of the "Judicial Power" in Statutory Interpretation, 1776–1806*, 101 Colum. L. Rev. 990, 1055 (2001).

The first Congress did not contemplate that the federal courts would be empowered to exercise independent law-making authority. As Alexander Hamilton articulated, the courts "may truly be said to have neither force nor will, but merely judgment." The Federalist No. 78 (Alexander Hamilton) (Jacob E. Cooke ed., 1961); *see also* David F. Epstein, *The Political Theory of The Federalist* (2008). The All Writs Act was not intended to provide the courts with law-making power.

A review of the historical scholarship demonstrates that writ authority was a comparatively inconspicuous addition to the federal court system. The first Congress extensively deliberated several other aspects of the first Judiciary Act. *See generally*, Charles Warren, *New Light on the History of the Federal Judiciary Act of 1789*, 37 Harv. L. Rev. 49, 95 (1923). Yet there is virtually no evidence of debate about the All Writs Act. *Id.* at 49; Lonny Sheinkopf Hoffman, *Removal Jurisdiction and the All Writs Act*, 148 U. Pa. L. Rev. 401, 435–36 (1999). The statute's language, considered in association with the lack of any significant discussion on this point, demonstrates that the drafters intended to grant the federal courts only limited authority. *Id.* (stating "the notion that a federal court, once created, would be vested with writ power to aid its existing jurisdiction would have been considered unremarkable"). The statute ensured that the federal system was authorized to issue writs sufficient to preserve its own jurisdiction, which is

consistent with the understanding and experiences of the drafters in the courts of the day. *See* Henry J. Bourguignon, *The Federal Key to the Judiciary Act of 1789*, 46 S.C. L. Rev. 647, 672 (1995). Early judicial interpretations confirm the understanding that the All Writs Act did not confer the courts with plenary power to issue orders. *See McIntire v. Wood*, 11 U.S. 504, 505–06 (1813) (the courts' power to issue writs "is confined exclusively to those cases in which it may be necessary to the exercise of their jurisdiction"); *Smith v. Jackson*, 22 F. Cas. 575 (C.C.N.D.N.Y. 1825).

The Supreme Court's more recent interpretations continue to view the All Writs Act, 28 U.S.C. § 1651(a), as only "a residual source of authority." *United States v. Zavalidroga*, 2 F. App'x 787, 788 (9th Cir. 2001) (citing *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985)). Today, courts are clear that the All Writs Act "does not give the district court a roving commission" to enlist third parties into law enforcement. *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). Rather, as the Ninth Circuit recognizes, the All Writs Act applies where there is an unmistakable "gap to fill" in a congressional statutory regime. *In re U.S. for an Order Authorizing the Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1145 & n.26 (9th Cir. 2003).

Courts consistently reject efforts like this one to use the All Writs Act to "issue supplemental orders to effectuate valid orders or warrants [that] constitute an additional invasion of privacy." *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 579 (D. Md. 2011). The historical interpretation of the All Writs Act is irreconcilably inconsistent with the position the government puts forward today.

V. THE GOVERNMENT CANNOT USE THE ALL WRITS ACT TO REWRITE STATUTORY AUTHORITY CONTROLLING THE GOVERNMENT'S ACCESS TO ELECTRONICALLY STORED INFORMATION

Today, although the All Writs Act facilitates extraordinary remedies under very particular circumstances, the section incorporates fundamental limitations that are

consistent with the Judiciary Act's original purpose. Specifically, the Act is considered a "residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau*, 474 U.S. at 43. Although the All Writs Act empowers federal courts to issue certain types of remedies, "it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *Id.* Therefore, "[w]here a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling." *Id.*; *Carlisle v. United States*, 517 U.S. 416, 429 (1996) (same); *Plum Creek*, 608 F.2d at 1289. The analysis must proceed under the relevant statute and not the All Writs Act. *See In re U.S. for an Order Authorizing the Roving Interception of Oral Commc'ns*, 349 F.3d at 1145 & n.26.

Pennsylvania Bureau illustrates the operation of this principle. In *Pennsylvania Bureau*, the Court considered district court orders that required U.S. Marshals to transport state prisoners to the federal trial courts to provide testimony. 474 U.S. at 35. The Court recognized that a statute, 28 U.S.C. § 2243, required prisoner transport by the "custodian," meaning the state prisons. *Id.* at 39. The Court rejected the argument that the All Writs Act allowed the district court to engage in "'creative' use of federal judicial resources to alleviate the drain on States' fisc" in light of the statute. *Id.* at 40. Holding that the All Writs Act could not support such an order, the Court recognized that the statute "expressly commands the custodian to bring his prisoner to the court, but extends this duty to no other." *Id.* at 39.

Here, the government has attempted to sidestep this crucial limitation. Specifically, the government argues that because there is no statute precluding it from forcing Apple to create government-specific software, it can demand the software under the All Writs Act instead. That is not—and cannot be—the test. The All Writs Act "does not authorize [federal courts] to issue ad hoc writs." *See id.* at 43. Indeed, just this week, Judge Orenstein rejected the government's argument in another case where the government

sought to force Apple to bypass the passcode on an Apple device.[5] Judge Orenstein held that "the established rules for interpreting a statute's text constrain me to reject the government's interpretation that the AWA empowers a court to grant any relief not outright prohibited by law." *Id.*

Other rulings have reached this same conclusion in analogous contexts.[6] Most notably, *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & Trap & Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) rejected the government's argument that the All Writs Act empowers a court to require a cell phone provider to furnish the government with a suspect's location. Observing that Congress had enacted two statutes, ECPA and CALEA, to govern this subject matter, the court explained:

> The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration. Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority.

Id. at 326.

Here, two statutes, CALEA, 47 U.S.C. § 1001 et seq., and ECPA, 18 U.S.C. §§ 2701–2719, already provide extensive rules that govern access to electronically communicated and stored information. For decades, Congress has responded to new technology and new threats to privacy and public safety with a network of carefully

---

[5] *In re Order Requiring Apple, Inc. To Assist in the Execution of a Search Warrant Issued by This Court*, No. 1:15-mc-01902-JO (E.D.N.Y. Feb. 29, 2016), ECF No. 29 at 1.

[6] *See In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d at 580 ("the All Writs Act cannot be used to circumvent the safeguards set in place by existing law"); *In re U.S. for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006) (same); *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d at 583 ("The government simply cannot use the All Writs Act to circumvent the requirements of the Fourth Amendment and other statutes that already occupy the space.").

drafted statutes. CALEA and ECPA outline a complex regime controlling the government's power to access electronically stored and communicated information held by a range of service providers, including detailed provisions prescribing the entities on which design requirements can be imposed, and the physical and semantic boundaries that limit such assistance. These statutes "cover the field." Courts should not disrupt the careful balance that Congress has struck after years of hearings, study, and experience.

The Ninth Circuit limits the All Writs Act to authorize court orders where there is some "gap to fill" due to Congress's failure to consider an area of law. *In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d at 1145 & n.26. Here, there are no gaps. Indeed, there are few areas of law in which Congress has provided more legislative guidance than the search and surveillance of electronically stored and communicated information—as well as the assistance third parties must provide law enforcement in obtaining this information.

Requiring Apple to redesign the iPhone operating system pursuant to an order issued under the All Writs Act to disable security features that prevent guessing or hacking the passcode reflects a profound disruption of Congress's carefully crafted regime. Such a mandate will have costs not just for Apple, but also for security and privacy globally. Because Congress can best weigh these difficult social issues, it is Congress's role to answer the contentious, difficult question of when manufacturers must redesign their products to undermine their own privacy protections. That decision should be left to the legislative power in Congress, not the courts' judicial power under the All Writs Act.

A. CALEA Specifies Who Must Assist Law Enforcement in Obtaining Electronic Information and What Assistance They Must Provide—and Specifically Excludes Decryption

In the area of protection of electronically communicated and stored information—and government's power to compel third parties to assist in collecting that information, Congress left no gaps. CALEA has been amended once and produced 850 pages of legislative history as well as a plethora of regulatory interpretations by the Federal

Communications Commission. *See, e.g.*, Communications Assistance for Law Enforcement Act, Report and Order, FCC 99-11 (Mar. 15, 1999); Communications Assistance for Law Enforcement Act, Order on Reconsideration, FCC 97-213 (Aug. 2, 1999); Communications Assistance for Law Enforcement Act, Second Report and Order, FCC 97-213 (Jan. 29, 1999).

CALEA provides a detailed statutory scheme that specifies which kinds of companies must assist the government in its surveillance orders and what assistance those companies must provide. Congress specifically excluded from its regulatory ambit firms such as Apple, decryption obligations (except in limited circumstances not present here), and, above all, design mandates.

First, CALEA explicitly states that it does not require telecommunication carriers to redesign their system configurations, stating that it "*does not authorize* any law enforcement agency or officer . . . to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by . . . any manufacturer of telecommunications equipment, or . . . to prohibit the adoption of any equipment, facility, service, or feature by . . . any manufacturer of telecommunications equipment." 47 U.S.C. § 1002(b)(1).

Second, in defining those types of firms subject to assist law enforcement, Congress decided that only "telecommunications carriers" would be obligated to make sure that their "equipment, facilities, or services" allow the government to intercept communications pursuant to a court order or other lawful authorization. *Id.* CALEA defines "telecommunications carrier" as an "entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." 47 U.S.C. § 1001(8)(A). Apple is not a common carrier, *i.e.*, a telephone company.

Rather, the Apple functionality at issue in this case would be classified under CALEA as an "information service," which is defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 1001(6). CALEA explicitly

"does not include persons or entities insofar as they are engaged in providing information services." 47 U.S.C. § 1001(8)(C)(i).

Third, Congress balanced privacy, security, and law enforcement needs by explicitly excluding from its obligations the duty to "decryp[t], or ensur[e] 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).

Finally, CALEA has set forth a procedure for expanding its coverage—which the government should first make use of. Section 1001(8)(B)(ii) states that the Federal Communications Commission can pull under its regulatory authority not simply providers of "wire or electronic communication" but also a "person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service." To the extent that law enforcement is seeking, for example, email or iMessage content from the iPhone in question, this provision provides a way for the FBI to go to the Commission to seek an extension of Apple's CALEA obligations. Indeed, the government already has done so, obtaining FCC authority to monitor VoIP and other internet-based communications. *In the Matter of Commc'ns Assistance for Law Enf't Act & Broadband Access & Servs.*, 20 F.C.C. Rcd. 14989, 14989 (2005), *on reconsideration in part*, 21 F.C.C. Rcd. 5360 (2006).

CALEA legislative history also shows Congress's decision to exclude Apple from any decryption requirements. Congress intended that collection and surveillance of electronic information should extend only to telecommunication providers, *i.e.*, telephone companies. "The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders." H.R. Rep. No. 103-827, pt. 1, at 18 (1994). Similarly, Congress did not intend CALEA to force firms to maintain an "encryption service for which [a carrier] does not retain the

ability to decrypt communications for law enforcement access." *See also id.* at 24.

B. ECPA Specifies Who Must Assist Law Enforcement in Obtaining Electronic Information and What Assistance They Must Provide—and Specifically Excludes Encrypted Information

ECPA sets forth a comprehensive set of rules that specifies the power of government to access stored electronic communications. It was the product of detailed study, robust debate, and compromise among competing interests. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004) (discussing background court disputes, Office of Technology Assessment Reports, congressional hearings, etc.); *see also* Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* 131 (1995) (discussing the formation of the Privacy and Technology Project of the ACLU and extensive consultations between privacy groups, technology experts, business groups, and congressional staff). ECPA's rules reflect Congress's balance between privacy and the needs of law enforcement, requiring certain types of firms to provide access to records that they store or possess. These rules refrain from requiring firms such as Apple from developing new technologies to undermine its own consumer privacy protections or to assist government in decryption.

Under ECPA, Apple must assist the government in obtaining records related to the iPhone stored on Apple's servers. Presumably, it has already provided access and assistance to the government with respect to information it possesses. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209–13 (2004). However, ECPA obligations only extend to records that are, in fact, stored by an electronic communication service provider or remote computing service provider. ECPA excludes from this obligation "information that an individual stores to his hard drive or cell phone [because it] is not in electronic storage under the statute." *Garcia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012). *See also Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1205 (S.D. Cal. 2008) ("E-mails stored on the laptop computer are not" subject to ECPA); *In re iPhone*

Application Litig., 844 F. Supp. 2d 1040, 1057–58 (N.D. Cal. 2012) (iPhones "d[id] not constitute 'facilit[ies] through which an electronic communication service is provided'" and thus ECPA does not cover them); *see also Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001) ("[Argument that] computers of users of electronic communication service, as opposed to providers of electronic communication service [conceivably subject to ECPA] [be] considered facilities through which such service is provided. . . . [is] destined to failure[.]").

ECPA places significant duties on Apple to assist law enforcement, but the government seeks more than ECPA permits. The government reads the All Writs Act "to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration." *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d at 326.

* * *

Congress, through the democratic process, has weighed and balanced these difficult concerns and created a comprehensive statutory regime, consisting in CALEA and ECPA. That regime—not the All Writs Act—should control.

VI. THE GOVERNMENT'S DEMAND WOULD IMPOSE AN UNREASONABLE BURDEN ON BOTH APPLE AND ITS USERS

The All Writs Act "may not impose an undue burden on a company enlisted to aid the government." *In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d at 1148 (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 172 (1977)). Nor may the All Writs Act create "disruption to [a third party's business] operations." *In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d at 1145. *No* court has *ever* looked to the All Writs Act to require a private corporation to develop new, costly technology that creates serious financial burdens, radically disrupts its business plan and disrupts its consumers' long-held privacy and

security expectations. Courts have resisted the government's attempts to use the All Writs Act to collect data using newer, more intrusive technologies. For instance, courts have rejected its use to obtain the real-time acquisition of prospective cell site information absent probable cause, concluding that such reliance "invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with . . . the extent of [judicial] authority." *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d at 326; *see also In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d at 578 ("The government [seeks] . . . precise [cell phone] location information under the All Writs Act. This may be the most troubling position the government has taken in pursuit of this precise location data") (internal citations omitted).

Congress's restraint in dictating design features stems from the risks such requirements pose not just to individual privacy, but to security in general. Such requirements threaten the security of information held by individuals, private firms and corporations, and, indeed, by our own local, state, and federal government, many of whom use iPhones to protect confidential information.

Adding custom mechanisms for law enforcement to access software systems, even if they are not, strictly speaking, 'back doors', creates a variety of technical risks to the security of the overall system. In particular, building the new features required by the Apple Order has uncertain consequences for the security of Apple's iOS environment overall. If Apple writes the code and gives it to the FBI to use, some or all of the code may fall into malicious hands. Whereas, if the code is executed within Apple's secure facilities, the connection between the FBI and Apple could become a target for attack. H. Abelson et al., *Keys under doormats: mandating insecurity by requiring government access to all data and communications*, Journal of Cybersecurity, 1–11 (2015). A thorough analysis of these risks would depend on the precise implementation approach chosen by Apple, but it is not clear how this Court could monitor the security exposure

created by the system as it operates.

Indeed, government's investigatory tools can be and have been misused. *See* Susan Landau, *Surveillance Or Security?: The Risks Posed by New Wiretapping Technologies* (2010). Security experts understand that the use of product update channels, to undermine device security in support of government access poses a serious security threat for three related reasons:

First, establishing a general practice of signing code—whose purpose is unrelated to the product's function and only for the benefit of law enforcement—will provide a vector for attacking cell phones. Requiring new updates pushed by law enforcement will put new pressure on the update cycle and risk diverting developers' attention from the core security of the product.

Second, software updates are essential to maintaining the security of devices and networks as new threats emerge. Their utility depends upon consumer trust that the software delivered improves their product. The use of update channels to open up vulnerabilities in response to law enforcement requests will undermine trust in updates.

Finally, orders to disable aspects of a cryptographic implementation, signal to the industry that investments in robust security may be ill-advised and costly, as they will require countless hours to redesign after the government comes knocking. Apple may have the resources to continue deploying strong encryption, but other companies with fewer resources may be incentivized to build systems ready-made for government access. Yet a technical vulnerability designed to ease law enforcement access also lets in anyone who can find it.

The delicate policy choices at issue are underscored by the number of former National Security, Intelligence, and Defense officials who have come out in support of robust "end-to-end unbreakable encryption" (*Gen. Michael Hayden Gives an Update on the Cyberwar*, Wall St. J. (Feb. 9, 2016), http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153), because "the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the

device, server and enterprise level without building in means for government monitoring." Mike McConnell et al., *Why the fear over ubiquitous data encryption is overblown*, Wash. Post (July 28, 2015), https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

Moreover, an additional set of third parties also risk facing burdens in this case: users of Apple products. Users may be at additional security risk as a result of the proliferation or mistaken use of the software being created under the Apple Order. Of course both Apple and the FBI will take care to avoid misuse of the software created here, but we have no means within this proceeding of carefully evaluating these burdens. In the meantime, users will have reason to wonder whether either Apple or the FBI has introduced vulnerabilities into the iOS environment.

The government's requested order here raises the question how the court should evaluate the cost of mandating security design not simply to Apple—but upon society and, indeed, the entire global economy. The fact that All Writs Act jurisprudence offers no guidance on this question strongly suggests that the court has entered territory much better suited for the democratic policymaking process of a legislature.

VII. NEITHER NEW YORK TELEPHONE NOR THE OTHER CASES THE GOVERNMENT CITES CAN SUPPORT THE APPLE ORDER

In the government's motion to compel and its underlying application for the Apple Order, the government relies heavily on *New York Telephone*. 434 U.S. at 174–75. However, that case cannot support the weight the government puts on it.

New York Telephone recognized that the order at issue in that case posed essentially no burden on the telephone company's ongoing operations. *Id.* ("Certainly the use of pen registers is by no means offensive to it. The Company concedes that it regularly employs such devices without court order for the purposes of checking billing operations, detecting fraud, and preventing violations of law."). In contrast, there is every indication that the Apple Order represents a significant outlay of time, expense, and risk to Apple. *Cf. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this*

Court, 2015 WL 5920207, at *5 ("there is nothing in the record to suggest that Apple has or wants the ability to defeat customer-installed security codes to access the encrypted data that its customers store on Apple devices after purchasing them."); *id.*, Case No. 15-1902 (E.D.N.Y. Feb. 29, 2016), ECF No. 29 at 38–44 (finding that requiring Apple to bypass an iPhone passcode would place an unreasonable burden on Apple including reputational harm, financial harm, burdens on Apple's ability to compete in the market, and a burden on Apple's ability, as a private entity, to avoid doing what it finds to be offensive).

Apple has submitted evidence that the creation, design, validation and deployment of the software necessary to comply with the Apple Order would take six to ten experienced Apple engineers and employees dedicating a substantial period of time for a minimum of two weeks.[7] Additionally, such deployment must occur at a secure, isolated facility to minimize the probability of a security leak.[8] Beyond this, to prevent the possibility that the code might get into the wrong hands and/or to accommodate additional government requests, Apple must maintain and house the government-specific operating system by taking the same levels of precautions needed to protect Apple's most sensitive trade secrets.[9] The Apple Order requires Apple to violate design decisions that it made intentionally to secure the device.[10] Under these circumstances, *New York Telephone* cannot support the Apple Order.

The burdens imposed on Apple—and the risks to the public's safety and privacy—are unlike other orders issued under the All Writs Act authority. The implications of

---

[7] Decl. of Erik Neuenschwander in Supp. of Apple Inc.'s Mot. to Vacate Order Compelling Apple, Inc. to Assist Agents in Search and Opp'n to Gov't's Mot. to Compel Assistance ("Neuenschwander Decl.") ¶ 22, Case No. 16-10 (C.D. Cal. Feb. 25, 2016), ECF No. 16-33.

[8] *Id.* ¶¶ 36–37.

[9] *Id.* ¶¶ 47–49. *See also* Decl. of Lisa Olle in Supp. of Apple Inc.'s Mot. to Vacate Order Compelling Apple, Inc. to Assist Agents in Search and Opp'n to Gov't's Mot. to Compel Assistance ¶¶ 13–14, Case No. 16-10 (C.D. Cal. Feb. 25, 2016), ECF No. 16-32.

[10] Neuenschwander Decl. ¶¶ 50–53.

disrupting the existing encryption system on iPhones are profound. These devices "place vast quantities of personal information literally in the hands of individuals." *Riley v. California*, 134 S. Ct. 2473, 2485 (2014). The software redesign the government demands in this case is arguably *more* privacy invasive. *See generally id.* at 2488–89 (recognizing privacy interests in cell phone content). While the facts of this case mute the privacy risks (the owner of the phone has consented, and the owner of the data is deceased), the background statutory scheme that must inform the court's use of the AWA does not contemplate, nor authorize, device manufacturers to assist the government in hacking lawfully purchased products to facilitate investigations.

Unlike the simple pen register at issue in *New York Telephone*, an iPhone facilitates myriad capabilities that rely on the storage of images, texts, browsing history, calendars, books, films, contact lists, banking information, and travel documentation. Using Apps or a browser, cell phones provide access to data stored remotely. The information stored on a device may concern the device's owner, as well as the owner's friends, family and acquaintances. Although both cases concern phones, a pen register stores numbers dialed from a particular phone line. In contrast, many cell phones "are in fact minicomputers that also happen to have the capacity to be used as a telephone." *Riley*, 134 S. Ct. at 2489.

Importantly, the Supreme Court only allowed the All Writs Act to include pen registers because such expansion was acceptable under Congress's existing electronic privacy regime. "It is clear that Congress did not view pen registers as posing a threat to privacy of the same dimension as the interception of oral communications and did not intend to impose Title III restrictions upon their use." *New York Telephone*, 434 U.S. at 168. Congress judged that the pen register's privacy infringement was not that significant and, therefore, made the decision *not* to regulate it. Here, however, Congress concluded the opposite, finding that mandating particular designs constituted such a threat to privacy and security that CALEA explicitly excludes it. *See* 47 U.S.C. § 1002(b).

As a private company, Apple is legally distinct from the public utility analyzed in *New York Telephone*. *See, e.g.*, *Michigan Bell Tel. Co. v. United States*, 565 F.2d 385,

389 (6th Cir. 1977) ("It is to be emphasized that a telephone company is no ordinary third party. It is a public utility, enjoying a monopoly in an essential area of communications."); *In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same). The government does not have the authority to conscript the services of a private company like Apple as it does to conscript the services of a highly regulated public utility. Case No. 15-1902 (C.D. Cal. Feb 29, 2016), ECF No. 29 at 31–32 ("[U]nlike the telephone company—'a highly regulated public utility with a duty to serve the public,'—Apple is a private entity with no greater duty to serve the public than any other business.") (internal citation omitted).

The other cases the government cites are readily distinguishable. In *United States v. Hall*, 583 F. Supp. 717, 721 (E.D. Va. 1984), the credit card records were already maintained by the company and could be generated by "punching a few buttons" and were in the company's possession. *See also In re Application of U.S. for an Order Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) ("the only cooperation required by the apartment complex is merely to provide access to surveillance tapes already in existence, rather than any substantive assistance, and nothing more."). The additional authority cited by the government acknowledges that the All Writs Act "do[es] not provide authority for [the court] to enter the requested order." *In re U.S. for an Order Directing a Provider of Commc'ns Servs. to Provide Tech. Assistance to Agents of the U.S. Drug Enf't Admin.*, 2015 WL 5233551, at *4 (relying on alternative authority). These cases underscore that the All Writs Act does not support the burdensome and intrusive nature of the Apple Order. *Cf. Plum Creek*, 608 F.2d at 1290 ("This circuit has never held that the district court has such wide-ranging inherent powers that it can impose a duty on a private party when Congress has failed to impose one.").

///

///

According to Apple, software on the iPhone that is the subject of the Apple Order was designed to optimize security, a core attribute of its functionality.[11] There may be private information on any iPhone that is more extensive, personal, and all-encompassing than almost any other owned object. It is a fair assumption that most cell phones also include information about those with whom the owner has communicated. To ask Apple to create code that unravels that security threatens harm to both Apple and the public interest. *Cf. In re U.S. for an Order Authorizing the Roving Interception of Oral Commc'ns*, 349 F.3d at 1145 ("The obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business . . . .").

This case raises important concerns for private enterprise, innovation, privacy, and constitutional rights more broadly. If upheld, the Apple Order will convert Apple into a state actor insofar as it will be compelled to participate in this search as an "agent or instrument of the Government." *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614–15 (1989). To the extent these requests become routine, they raise concerns that companies will be required to design their products to support governmental access going forward. This would have the effect of giving the government de facto control over technical design while also permanently converting Apple and other private companies into state actors, subjecting them to a range of constitutional duties and restraints that normally do not apply to private entities, including those imposed by the Fourth Amendment. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 135–36 (2013). This would have a host of consequences for individuals' rights to be secure against unreasonable searches, data security, and scientific and technical advance more generally while also dramatically altering relationships between technology companies and their consumers. As both a constitutional matter and

[11] Hanna Decl. Ex. D, Case No. 16-10 (C.D. Cal. Feb. 25, 2016), ECF No. 16-5.

a policy matter, allowing the federal government *de facto* control over the design of technology is therefore an extraordinary remedy that requires careful consideration. CALEA reflects a legislative view that this remedy is appropriate in a very narrow circumstance. The All Writs Act by contrast does not reflect any legislative wisdom suggesting that broader government control over technology companies, their products, and their consumer market is appropriate or constitutional.

VIII. CONCLUSION

For the reasons described above, the Court should deny the government's motion to compel and vacate its February 16, 2016 order.

Dated: March 3, 2016

DURIE TANGRI LLP

By: Mark Lemley /MAF
MARK A. LEMLEY

Attorneys for *Amicus Curiae*
Law Professors

Janet Ainsworth
John D. Eshelman Professor of Law
Seattle University

Jordan (Jody) M. Blanke
Ernest L. Baskin, Jr. Distinguished Professor of Computer Information Systems and Law Stetson School of Business & Economics Mercer University

Annemarie Bridy
Professor, University of Idaho College of Law

Dan L. Burk
Chancellor's Professor of Law
University of California, Irvine

Adam Candeub
Professor of Law, Director, IP, Information, and Communications Law Program
Michigan State University College of Law

Michael A. Carrier
Distinguished Professor
Rutgers Law School

Megan M. Carpenter
Professor of Law
Co-Director, Center for Law and Intellectual Property (CLIP)
Faculty Director, IP and Technology Law Clinic
Faculty Director, Entrepreneurship Law Clinic
Texas A&M University School of Law

Anupam Chander
Professor
University of California, Davis, School of Law

Andrew Chin
Associate Professor
University of North Carolina School of Law

A. Michael Froomkin
Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law
University of Miami

David Gray
University of Maryland
Francis King Carey School of Law

Woodrow Hartzog
Associate Professor
Samford University's Cumberland School of Law

Stephen E. Henderson
Judge Haskell A. Holloman Professor of Law
The University of Oklahoma

Margot E. Kaminski
Assistant Professor
The Ohio State University Moritz College of Law Affiliated Fellow, Information Society Project at Yale Law School

Raymond Ku
Professor of Law
Case Western Reserve University School of Law

Mark A. Lemley
William H. Neukom Professor, Stanford Law School Director, Stanford Program in Law, Science, and Technology Senior Fellow, Stanford Institute for Economic Policy Research partner, Durie Tangri LLP co-founder, Lex Machina Inc.

Richard A. Leo, Ph.D., J.D.
Hamill Family Professor of Law and Psychology
University of San Francisco

David S. Levine
Visiting Research Collaborator, Center for Information Technology Policy, Princeton University; Associate Professor and Chair, Faculty Development, Elon University School of Law; Affiliate Scholar, Center for Internet and Society, Stanford Law School

Yvette Joy Liebesman
Associate Professor of Law
Saint Louis University School of Law

Deirdre K. Mulligan
Associate Professor of Law
School of Information
University of California at Berkeley

Ira Steven Nathenson
Professor of Law
St. Thomas University School of Law

Blake E. Reid
Assistant Clinical Professor
Colorado Law

Neil Richards
Professor of Law
Washington University

Jorge R. Roig
Associate Professor of Law
Charleston School of Law

Ira Rubinstein
Senior Fellow and Adjunct Professor
Information Law Institute
New York University School of Law

Victoria Schwartz
Associate Professor
Pepperdine University School of Law

Robert H. Sloan
Professor and Department Head
University of Illinois at Chicago Dept. of Computer Science

Stephen F. Smith
Professor of Law
University of Notre Dame

Daniel J. Solove
John Marshall Harlan Research Professor of Law
George Washington University Law School

Gerry Stegmaier
George Mason University School of Law

Daniel J. Weitzner
Principal Research Scientist, MIT Computer Science and Artificial Intelligence Lab, Director, MIT Internet Policy Research Initiative

Michael Zimmer, PhD
Associate Professor and PhD Program Director, School of Information Studies
Director, Center for Information Policy Research University of Wisconsin-Milwaukee

PROOF OF SERVICE

I am a citizen of the United States and resident of the State of California. I am employed in San Francisco County, State of California, in the office of a member of the bar of this Court, at whose direction the service was made. I am over the age of eighteen years, and not a party to the within action. My business address is 217 Leidesdorff Street, San Francisco, CA 94111.

On March 3, 2016, I served the following documents in the manner described below:

***AMICUS CURIAE* BRIEF OF LAW PROFESSORS IN SUPPORT OF APPLE, INC.**

☐ (BY U.S. MAIL) I am personally and readily familiar with the business practice of Durie Tangri LLP for collection and processing of correspondence for mailing with the United States Postal Service, and I caused such envelope(s) with postage thereon fully prepaid to be placed in the United States Postal Service at San Francisco, California.

☐ (BY MESSENGER SERVICE) by consigning the document(s) to an authorized courier and/or process server for hand delivery on this date.

☐ (BY FACSIMILE) I am personally and readily familiar with the business practice of Durie Tangri LLP for collection and processing of document(s) to be transmitted by facsimile and I caused such document(s) on this date to be transmitted by facsimile to the offices of addressee(s) at the numbers listed below.

☐ (BY OVERNIGHT MAIL) I am personally and readily familiar with the business practice of Durie Tangri LLP for collection and processing of correspondence for overnight delivery, and I caused such document(s) described herein to be deposited for delivery to a facility regularly maintained by Federal Express for overnight delivery.

☒ BY ELECTRONIC SERVICE: By electronically mailing a true and correct copy through Durie Tangri's electronic mail system from mfeldman@durietangri.com to the email addresses set forth below.

☐ (BY PERSONAL DELIVERY) I caused such envelope to be delivered by hand to the offices of each addressee below.

On the following part(ies) in this action:

Eric David Vandevelde
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071
2132297186

Fax: 2132296186
Email:
evandevelde@gibsondunn.com

Attorneys for Respondent Apple Inc.

Theodore J Boutrous, Jr.
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 900713197
2132297000

Fax: 2132297520

Email: tboutrous@gibsondunn.com

Attorneys for Respondent Apple Inc.

Jeffrey G Landis
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
2022963585
Fax: 2027065298
Email: jeff@zwillgen.com

Attorneys for Respondent Apple Inc.

Theodore B Olson
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 200365306
2029558668
Fax: 2025309575
Email: tolson@gibsondunn.com

Attorneys for Respondent Apple Inc.

Nicola T Hanna
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 926124412
9494513800
Fax: 9494514220
Email: nhanna@gibsondunn.com

Attorneys for Respondent Apple Inc.

Marc J Zwillinger
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036
2022963585
Fax: 2027065298
Email: marc@zwillgen.com

Attorneys for Respondent Apple Inc.

Allen W Chiu
AUSA Office
of US Attorney
National Security Section
312 North Spring Street Suite 1300
Los Angeles, CA 90012
2138942435
Fax: 2138946436
Email: allen.chiu@usdoj.gov

Attorneys for USA

Tracy L Wilkison
AUSA Office of US Attorney
Chief, Cyber and Intellectual Property
Crimes Section
312 North Spring Street 11th Floor
Los Angeles, CA 900124700
2138940622
Fax: 2138940141
Email: tracy.wilkison@usdoj.gov

Attorneys for USA

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on March 3, 2016, at San Francisco, California.

MICHAEL A. FELDMAN