ANDREW P. BRIDGES (CSB No. 122761)
abridges@fenwick.com
DAVID L. HAYES (CSB No. 122894)
dhayes@fenwick.com
TYLER G. NEWBY (CSB No. 205790)
tnewby@fenwick.com
CIARA N. MITTAN (CSB No. 293308)
cmittan@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Tel: (415) 875-2300
Fax: (415) 281-1350

Attorneys for *Amici Curiae*, AVG Technologies, the Computer & Communications Industry Association, Data Foundry, Golden Frog, Internet Association, and the Internet Infrastructure Coalition

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OFAN 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) **BRIEF OF *AMICI CURIAE* AVG TECHNOLOGIES, THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, DATA FOUNDRY, GOLDEN FROG, THE INTERNET ASSOCIATION, AND THE INTERNET INFRASTRUCTURE COALITION 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** Date: March 22, 2016 Time: 1:00 p.m. Dept: 3 or 4 – 3rd Floor Judge: Hon. Sheri Pym

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continuation)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(Continuation)

Page(s)

CASES

STATUTES

TABLE OF AUTHORITIES
(Continuation)

Page(s)

CASES

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(Continuation)

Page(s)

CASES

INTERESTS OF AMICI CURIAE

Amici are technology companies or entities that represent or support technology companies who share a unified interest in advocating a principled interpretation of the All Writs Act that protects the ability of technology companies to develop and maintain secure products and services. AVG Technologies is a leading provider of software services to secure devices, data and people. Data Foundry is one of the first 50 ISPs in the United States, whose data centers have supported thousands of enterprise companies in every industry, including high performance computing, energy, financial services, healthcare and technology. Golden Frog was founded to build tools that help preserve an open and secure Internet experience while respecting user privacy. The Computer & Communications Industry Association (CCIA) represents over 20 companies in the computer, Internet, information technology, and telecommunications industries, ranging in size from small entrepreneurial firms to some of the largest companies in these industries. The Internet Association, representing the interests of 35 leading Internet companies and their global community of users, is dedicated to advancing public policy solutions that strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. The Internet Infrastructure Coalition (i2Coalition) is the non-profit voice of companies from the Internet infrastructure industry. As diverse stakeholders in the Internet, technology, and security industries, *Amici* have a substantial interest in this proceeding and its potential unprecedented impact.

INTRODUCTION

In response to the clear and present danger posed by profit-minded criminal hackers, thieves and state-sponsored organizations, many American businesses have implemented strong, user-controlled security to protect both their businesses and their customers from harm. Apple Inc. is one such company, having encrypted user data on its latest iPhone models by default, putting the decryption key in the

hands of the users alone, and creating technical safeguards to deter malicious actors from trying to break into users' phones. The government now seeks a court order under the All Writs Act to compel Apple to create and implement new software to undermine these security features, despite Congress's having enacted a statutory scheme that declined to grant the government that power. The government's interpretation of the All Writs Act, if adopted, could empower it to compel numerous companies to disable security features ingrained in their products against their interests, all without statutory authority. Indeed, the government acknowledges that it has sought and continues to seek All Writs Act orders to compel Apple in numerous other cases. This effort offends principles of separation of powers and could threaten the security of technology businesses and their users. *Amici* therefore support Apple's motion to vacate this Court's February 16, 2016 order compelling Apple Inc. to assist the government, as the "reasonable technical assistance" that the Order requires is not reasonable at all.

Scores of diverse technology companies, especially business- and consumer-facing Internet companies, relentlessly strive to make their customers' most sensitive information increasingly secure in the face of ever-growing threats from a wide variety of malefactors. For many technology companies, the quality of the security they employ is a core feature and influences whether customers will use their services or purchase their products. In response to security threats and consumer demand, some businesses have deliberately designed their products and services with security so strong that they can never access the sensitive data their customers have encrypted. Customers of these products include government agencies, defense contractors, financial institutions, healthcare providers, public utilities, airlines, railroads, manufacturers, and individual citizens. The government asks Apple (and its employees) to undertake labor Apple is unwilling to do, for an objective Apple perceives—with good reason—as harmful: to design and write new software to defeat important security protections in an Apple product. By doing so,

the government demands that Apple deliberately compromise one of the most widely relied-on products in the world.

The government professes that this request is an isolated request about a single phone in a single investigation. But, the government does not deny that it is already seeking similar orders from other courts around the country. If it prevails on its sweeping interpretation of the All Writs Act here, it is almost certain to seek to leverage that outcome in an effort to conscript a wide range of businesses and industries to achieve its ends through means foreclosed by Congress.[1] Many such efforts are likely to take place in *ex parte* proceedings, as was the case here, with no advance opportunity for the affected businesses to be heard. Smaller companies without the resources of Apple are more likely to quickly cave to the government's demands in those cases, choosing the burden of creating new technology that undermines their products' security over the threat of a contempt order.

Over the 227-year history of the All Writs Act there is no precedent for what the government wants to do here—use a court's ancillary authority to conscript a private enterprise against its will to create new technology that undermines a core feature of its own products and security. To the contrary, earlier this week on February 29, 2016, United States Magistrate Judge Orenstein soundly rejected the government's attempt to use the All Writs Act to compel Apple to do far less than what the government seeks here, finding that "the extraordinary relief [the government] seeks cannot be considered 'agreeable to the usages and principles of law.'" *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, 15-MC-1902 (JO), 2016 WL 783565, at *7

[1] In response to questioning by the House Judiciary Committee on March 1, 2016, FBI Director James Comey stated that "of course" the FBI would demand assistance in unlocking devices in future cases "if the All Writs Act is available to us." United States. Cong. House. Committee on Judiciary. *Encryption Tightrope: Balancing Americans' Security and Privacy*, Mar. 1, 2016, 114th Cong. (available at http://www.c-span.org/video/?405442-1/hearing-encryption-federal-investigations)

(E.D.N.Y. Feb. 29, 2016) (the "*In re Order*"). There, the government sought Apple's assistance in unlocking an unencrypted password-protected iPhone that lacked many of the security features that the iPhone 5c in this case possesses. It did not require Apple to help the company defeat encryption on the device. *Id.* at *5. Even then, the court held the "assistance" the government sought exceeded the Court's statutory authority under the All Writs Act and was not supported by a proper balancing of discretionary factors the Supreme Court established in *United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977). The result should be no different here.

BACKGROUND

Apple's brief on its motion to vacate summarizes the procedural background leading to the Court's issuance of the Order, which *Amici* will not repeat. *See* Apple's Motion at 10-14. On February 16, 2016, this Court issued an order compelling Apple to assist in the manner the government proposed. Order Compelling Apple, Inc. to Assist Agents in Search, 5:15-mj-00451-DUTY-1, Dkt. No. 19 (C.D. Cal. Feb. 16, 2016) ("Order"). The Order compels Apple to provide what the government deems "reasonable technical assistance" to obtain data on an encrypted device that Apple manufactured and sold, but does not possess. Order at *2; *see* Government Application, 5:15-mj-00451-DUTY-1, Dkt. 18, at *2 (C.D. Cal. Feb. 16, 2016) (hereinafter "Application"). To do so, the "government requests that Apple be ordered to provide the FBI with a signed iPhone software file, recovery bundle or other software image file ("SIF") that can be loaded onto the SUBJECT DEVICE." Application at *6. This proposed SIF would have "three important functions." *Id.* at *7. First, this SIF would "bypass or disable the auto-erase function" allowing for "multiple attempts at the passcode." *Id.* Second, this SIF would "enable the FBI to submit passcodes" electronically. *Id.* Third, the SIF would remove the passcode delay function. *Id.*

ARGUMENT

I. THE COURT'S ORDER IS AN IMPROPER AND UNPRECEDENTED EXPANSION OF SCOPE OF THE ALL WRITS ACT.

The government contends that its application to compel Apple to create new software to defeat strong security features Apple has architected into one of its core products is the type of "assistance" courts have typically authorized under the All Writs Act. That is false. The government's position is belied by both the historical context in which All Writs Act was enacted and how courts have applied it since the nation's founding. For 227 years, the language of the statute, "courts. . . may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law,"[2] 28 U.S.C. § 1651, has been applied narrowly to require companies to provide meager assistance in the execution of a law enforcement order only where doing so does not undermine the company's business. It is not a fountainhead for the authorization of any government demand related to an investigation, and it has never been applied to conscript a company and its employees, by their compelled labor and ingenuity, to invent new technologies to counteract and undermine their own products and business. As Judge Orenstein's order concluded, "the government posits a reading . . . so expansive—and in particular, in such tension with the doctrine of separation of powers—as to cast doubt on the AWA's constitutionality if adopted." *In re Order*, 2016 WL 783565, at *7. Judge Orenstein's analysis applies with even greater force here, where the government seeks to compel Apple to create new software that undermines core security features.

[2] As chronicled in Judge Orenstein's February 29, 2016 order, the text of the All Writs Act has been amended only twice in succeeding centuries since its adoption, and never in any substantive way. *See In re Order*, 2016 WL 783565, at *6.

A. The Historical Context in Which the All Writs Act Was Enacted Weighs Against the Government's Broad Interpretation.

The historical context from which the All Writs Act arose supports a limited reading of orders that are "agreeable to the usages and principles of law." The All Writs Act was enacted on September 23, 1789 as part of the Judiciary Act in the First Congress of the new United States.[3] The next day, Congress approved the Bill of Rights, including the Fourth Amendment, which was "most immediately the product of contemporary revulsion against a regime of writs of assistance." *Stanford v. Texas*, 379 U.S. 476, 482 (1965).

A writ of assistance, more commonly called a "writ of aid," was a written order issued by a Court, authorizing wide-ranging searches of anyone, anywhere, and anytime without their being suspected of a crime. Writs of assistance "could be used to enlist the aid of any officer of the crown in conducting a search of a dwelling, shop or warehouse for smuggled goods."[4] These "hated writs" spurred colonists towards revolution[5] and directly motivated the creation of the Fourth Amendment.[6] Against this backdrop, Judge Orenstein correctly concluded that interpreting the All Writs Act as authorizing orders conscripting private citizens into the service of the government in the interest of providing "assistance" is not "agreeable to the usages and principles of law."[7]

---

[3] Federal Judiciary Act of 1789, ch. 20, 1 Stat. 73, 81-82.

[4] James M. Farrell, "The Child Independence is Born: James Otis and Writs of Assistance," in Rhetoric, Independence and Nationhood, ed. Stephen E. Lucas, in Vol. 2 of *A Rhetorical History of the United States: Significant Moments in American Public Discourse*, 6 ed. Martin J. Medhurst (Mich. State Univ. Press, forthcoming).

[5] *Stanford v. Texas*, 379 U.S. 476, 484 n.13.

[6] *See, e.g., Frank v. Maryland*, 359 U.S. 360, 364 (1959); *Boyd v. United States*, 116 U.S. 616, 625 (1886). *See also* William John Cuddihy, *The Fourth Amendment: Origins And Original Meaning* (2009).

[7] Indeed, despite the commercial availability of unpickable locks during the first half-century following the enactment of the All Writs Act, there is no record in the case law of courts ordering the manufacturers of those devices to defeat their own locks in aid of law enforcement. *See, e.g.*, Joseph Bramah, "A Dissertation on the

B. Courts Have Not Applied the All Writs Act to Compel Companies to Create New Technology, Much Less Where It Undermines Fundamental Features of Their Businesses or Products.

Relying principally on *New York Telephone*, the government asserts that its request is consistent with the historical use of the All Writs Act, describing the *ex parte* order as requiring Apple to provide only "reasonable technical assistance."[8] *See* Order ¶ 1. But the government's request is both at odds with the facts and holding of *New York Telephone* and goes far beyond the historical kinds of "assistance" courts have ordered persons and businesses to provide under the All Writs Act. Courts have not applied the All Writs Act to require a business to invent new technology that did not previously exist and that the business would not otherwise create. And courts have certainly never ordered the creation of new technology that harms the privacy and security of a business and its customers.

In *New York Telephone*, the Supreme Court upheld a district court order directing a phone company to make two of its unleased phone lines available to assist the government's installation of a pen register on the line of a suspected bookmaker. 434 U.S. at 162-63. In evaluating the order, the Court applied a three-factor inquiry: (1) whether the company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled"; (2) whether the requested assistance would place an undue burden on a third party; and (3) whether the requested assistance is necessary to carry out the court's order. *Id.* at 174. Applying those factors, the Court held that the order was appropriate because: (1) the suspect was using the phone company's phone lines to facilitate an ongoing crime; (2) the company conceded that the effort involved in providing

---

Construction of Locks," in *Engineers* 150 (DK Press, 2012); Marc Weber Tobias, *Locks, Safes, and Security* 19 (Charles C Thomas Pub Ltd, 2nd ed. 2000).; Graham Pulford, *High-Security Mechanical Locks: An Encyclopedic Reference* 558, (Butterworth-Heinemann, 1st ed. 2007).

[8] *See* also, Application; *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 (E.D.N.Y. Oct. 9, 2015).

access to two unleased lines was "meager"; and (3) the government had no other means of installing a pen register without alerting the suspect. *Id.* at 174-75.

But the Court also considered another factor critical to the outcome of that case and equally critical here: whether the requested assistance was "offensive" to the company's business—that is, whether the business had a "substantial interest in not providing assistance." *Id.* at 174. In *New York Telephone*, providing the two unleased phone lines was not "offensive" to the phone company's business. It was a highly regulated public utility and regularly used pen registers for its own business purposes, including for customer billing and fraud detection. Whether that factor is part of the Court's undue burden analysis, as Judge Orenstein considered it, or whether it is a separate factor unto itself, it must be considered and is determinative here, as it was in *In re Order, Inc.*, 2016 WL 783565, at *21 (concluding that "the assistance the government seeks here . . . is, at least now, plainly 'offensive' to Apple) (quoting *N.Y. Tel. Co.*, 434 U.S. at 174).

1. Compelling a Company to Create Technology That Undermines its Product Security Is "Offensive" and Against the Substantial Interests of That Company

The government argues that Apple's resistance to complying with the Order is a "marketing strategy" and that forcing the company to defeat the protections it built into its phones does not amount to an undue burden on a substantial business interest. *See* Motion to Compel (Dkt. No. 1) at 17-18. This argument incorrectly describes the nature and gravity of Apple's interest—and the interest of other technology companies that build security into their products and services—in designing and selling secure products. It is also wrong as a matter of law.

American citizens, companies and the government face a daunting barrage of cyberattacks from diverse adversaries, including state-sponsored groups, organized hacking rings, and opportunistic individuals. Motion at 1. The consequences of suffering a significant data breach are severe for the affected customers and the businesses that are attacked. Companies, on average, face per capita costs of $217

for each person whose personally identifiable information has been compromised by a breach, and the costs rise each year. Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, Symantec and Larry Ponemon (May 30, 2015) (available at http://www-03.ibm.com/security/data-breach/). Worse, the steady drumbeat of reports of data breaches erodes consumer trust in the Internet economy and its technologies, threatening to stifle both growth and innovation.

To defend both their businesses and their customers' privacy and security against these threats, businesses have a substantial interest in building and maintaining strong security over their networks and the sensitive data their customers store on their products and services. Indeed, many businesses have responded to these risks and guidance from the government by investing heavily in people, equipment and software to build increasingly complex security into their businesses. Globally, corporate investment in improving information security has risen from an estimated $65.5 billion in 2013 to over $75 billion in 2015, and is projected to grow to over $90 billion in 2017. Gartner, Inc., "Forecast Analysis: Information Security, Worldwide, 2Q15 Update" (September 2015). The encryption Apple has built into its iOS devices is one prominent example of these efforts.

Technology companies therefore have a compelling interest in employing strong security measures to protect their customers' data from unauthorized access and misuse, including encryption, cryptographically-signed software updates,[9] password hashing and salting,[10] password lockouts,[11] and multi-factor

[9] Cryptographically signing software updates is a method used by Apple and other device manufacturers and software developers that prevents operating system software from being installed on a device unless it contains an encryption key that only the manufacturer or developer holds.

[10] Passwords are "hashed" using an established algorithm to change them from human-readable, so-called "plaintext" into unique encrypted strings of text like "5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8" (the sha-256 hash for 'password'). To make them more difficult to crack, small amounts of additional information called "salt" can be added. Therefore, even if someone attempted to brute force the encryption, or knew the hashing algorithm used, the decrypted information would not match the original plaintext (password).

authentication,[12] to name a few. Being compelled to invent vulnerabilities to undermine these measures is offensive to businesses, in ways that a telephone company allowing law enforcement to use a tool that the company itself regularly uses to combat fraud is not. The Court should vacate the Order on this basis alone.

Indeed, various arms of the Executive Branch have recognized the threats businesses and their customers face from cybercrime, and have encouraged, if not pleaded with, businesses to fortify their security, both to protect consumers' sensitive personal information from bad actors and to ensure confidence in an increasingly online economy. Three years ago, the President issued an Executive Order finding that cyber threats to critical infrastructure represent one of the most serious national and economic security challenges the nation must confront. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013). The White House's National Security Council has also spotlighted the threats cybercrime poses to the Internet economy, warning that "[p]ervasive criminal activity in cyberspace not only directly affects its victims, but can imperil citizens' and businesses' faith in these digital systems, which are critical to our society and economy." President Obama, "Strategy to Combat Transnational Organized Crime at *8 (July 2011) (available at https://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf).

The FBI also acknowledges the significance of the threats that cybercrime poses to American businesses, individuals, and the economy as a whole. In February 2012, the FBI's outgoing Executive Assistant Director overseeing cyber investigations worried: "I don't see how we ever come out of this *without changes in technology* or changes in behavior, because with the status quo, it's an

[11] A password lockout either temporarily or permanently prevents continued guessing of a password after a set number of failures.

[12] Multi-factor authentication is a method of authenticating an individual based on multiple pieces of information (e.g., a remembered password plus a code sent to a known mobile phone number or a number randomly generated).

unsustainable model. Unsustainable in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security." Devlin Barrett, "U.S. Outgunned in Hacker War," Wall Street Journal (Mar. 28, 2012). Despite that warning nearly four years ago, cyberattacks have increased relentlessly in number and scope, as has the cost to companies of responding to them. Just last week, Director Comey told Congress that the FBI continues "to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims." Statement Before the House Appropriations Comm., Subcomm. on Commerce, Justice, Science, and Related Agencies, (Feb. 25, 2016) (available at https://www.fbi.gov/news/ testimony/fbi-budget-request-for-fiscal-year-2017).[13]

Using both the carrot of education and the stick of civil enforcement actions, the Federal Trade Commission has also encouraged companies to build strong security features into their products and systems from the outset. In its guidance to businesses, the FTC has recommended that companies incorporate the principle of "Privacy by Design" into their practices, of which data security is a necessary pillar. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" at *22 (March 2012). It has also published data security guides for business encouraging companies to encrypt sensitive data, both while it is in transit and at rest. Federal Trade Commission, "Start with Security: A Guide for Business" at *6 (June 2015). The FTC has even encouraged companies to

[13] The FBI's Cyber Division routinely notifies businesses of cybersecurity threats, and has identified cyberattacks by groups affiliated with or sympathetic to terrorist groups. *See*, *e.g.*, Federal Bureau of Investigation Cyber Division Private Industry Alert, "Threat of Cyberterrorist and Hacktivist Activity in Response to US Military Actions in the Middle East," Sept. 24, 2014 (available at http://s3.documentcloud.org/documents/ 1306420/fbi-private-industry -notification-threat-of.pdf); see also "FBI Warns of ISIS-Inspired Cyber Attacks on 9/11 Anniversary," Sept. 11, 2015 (available at http://abcnews.go.com/US/fbi-warns-isis-inspired-cyber-attacks-911-anniversary/story?id=33684413).

"[c]onsider adding an 'auto-destroy' function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet," a feature remarkably similar to that which is before the Court here. *Id.* at 13. Above all, the FTC has recommended that companies continue to innovate and deploy technologies to protect their customers' sensitive data "such as encryption and anonymization tools." FTC, "Protecting Consumer Privacy" at *31. The FTC has also brought several civil enforcement actions against companies alleging their use of weak data security, including proprietary or incorrectly configured encryption, was an unfair or deceptive business practice. *See In the Matter of Henry Schein Prac. Sols., Inc., A Corp.*, 142-3161, 2016 WL 160609 (F.T.C. Jan. 5, 2016); *Federal Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015); *In the Matter of Fandango, LLC, A L.L.C.*, 2015-1 Trade Cas. (CCH) ¶ 17098 (F.T.C. Aug. 13, 2014); *In the Matter of Credit Karma, Inc., A Corp.*, 2015-1 Trade Cas. (CCH) ¶ 17099 (F.T.C. Aug. 13, 2014).

Thus, there can be no question that businesses that have made design choices to build security into their products and services have a substantial interest in those services that is not mere "marketing strategy."

2. An Order to Invent and Create New Technology to Assist Law Enforcement Is Unduly Burdensome, Particularly on Small and Nascent Technology Companies.

An order compelling a business to build technology to undermine strong security features is unduly burdensome by comparison to the minimal efforts and business impact that have previously been required of businesses under the All Writs Act. Indeed, in *New York Telephone*, the Court referred to the requested assistance as "meager." *Id.* at 174. This case is vastly different. Apple is being forced to invent and implement a new technology that doesn't yet exist, and that it would likely be forced to implement time and time again. As Apple explained in its Motion and accompanying declarations, acceding to the government's demand would require developing new secure facilities, hiring additional personnel, and

diverting resources from developing new products, all in the name of weakening security. Apple Inc.'s Motion to Vacate, 5:15-mj-00451-DUTY-1, at *13 (C.D. Cal. 2016) (hereinafter "Motion to Vacate").

There is no parallel to this type of burden in the All Writs Act case law. Instead, "assistance" has been limited to acts that companies conduct in the normal course of their business and that require minimal uses of company resources to provide access to existing records or facilities, including:

- ***Producing existing business records, often for the purpose of tracking fugitives***; *see, e.g.*, *United States v. Hall,* 583 F. Supp. 717, 721 (E.D. Va. 1984) (ordering bank to produce credit card transaction records, that could be generated by "punching a few buttons"); *United States v. Doe*, 537 F. Supp. 838, 840 (E.D.N.Y. 1982) (ordering a phone company to produce telephone toll records); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (same);
- ***Freezing assets and accounts to prevent the frustration of forfeiture and restitution orders***; *see, e.g., United States v. Yielding,* 657 F.3d 722 (8th Cir. 2011) (order preventing a restitution debtor from frustrating collection of the restitution debt); *United States. v. Simmons*, 07-CR-30, 2008 WL 336824, at *1 (E.D. Wis. Feb. 5, 2008) (temporary restraining order to freeze defendant's checking account); *United States v. Runnells*, 335 F. Supp. 2d 724, 725–26 (E.D. Va. 2004) (restraining defendants from diverting funds to avoid paying restitution);
- ***Turning over security camera footage***; *see, e.g., In re Application of United States for an Order Directing X to Provide Access to Videotapes,* No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (ordering a landlord to provide access to security camera videotapes);

- ***Ordering a defendant to reveal a password***; *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012) (order requiring defendant to provide password to encrypted computer seized pursuant to a search warrant); and
- ***Providing law enforcement access to existing and available telecommunications equipment to carry out wiretaps and pen/traps orders***; *See, e.g., N.Y. Tel. Co.*, 434 U.S. at 172; *In re Application*, 610 F.2d 1148, 1155 (3d Cir. 1979); *Application of U.S. for an Order Authorizing an In–Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1132 (9th Cir. 1980); *In re Application of U.S. for an Order Directing a Provider of Commc'n Servs. to Provide Tech. Assistance to Agents of the U.S. Drug Enforcement Admin.*, No. 15-1242, 2015 WL 5233551, at *5 (D.P.R. Aug. 27, 2015).

None of these cases imposed the same burden as the order requested by the government here would. Phone companies can easily implement trap and trace devices, and they maintain toll records for billing purposes. Credit card companies have customer records in their files for billing purposes. A landlord who already records his apartment common areas can provide access to those recordings. Tracing a call through an electronic device has no discernable burden and is effectively the same as a manual trace. None of these cases involved anything more than what a business already did in the normal scope of its business. However, compelling a company to invent a new technology by writing and testing software (a process that is creative, laborious, and expert) that does not yet exist is a distinction with a major difference. *See In re Order*, 2016 WL 783565, at *21 (finding that "bypassing a security measure that Apple affirmatively markets to its customers – is not something that Apple would normally do in the conduct of its own business" was unduly burdensome).

If giving the government the power to compel companies to invent and create

technology to suit the government's needs is burdensome to one of the world's most valuable companies, then it would be even more burdensome to the constellation of nascent and small technology and Internet companies that are driving the country's innovation economy. Faced with the potential for repeated demands for resources to weaken the security of their products, some companies may decide to close their doors, and innovators may choose not to launch new, innovative services. This concern is not an idle one; there is recent precedent of small, secure email service providers voluntarily shuttering their businesses in the face of court orders to provide the government with encryption keys that the *companies* controlled.[14] Worse, other companies may decide that leaving their services permanently insecure in order to ease their burden of complying with court orders is more economically viable. That result would lead to a persistence of the "status quo" of insecurity the FBI's Executive Assistant Director for Cyber worried about four years ago. *See* WSJ, "U.S. Outgunned in Hacker War."

The burden that would fall on small companies that lack the sizeable legal, technical, financial and human resources of Apple could be especially harsh, particularly if faced with numerous court orders. Unlike Apple, most information technology businesses are relatively small and operate on the edge of profitability in an intensely competitive market. The "assistance" sought here (which the government will surely repeat and expand in the future if allowed by this Court) could be detrimental to any small business faced with numerous demands to reverse or reopen the security measures the companies devoted substantial resources to building into their products. Thus, the government's position, if adopted, would present small companies with two unenviable choices: (1) build backdoors into

[14] *See* Ladar Levison, "Secrets, lies and Snowden's email: why I was forced to shut down Lavabit," The Guardian, May 20, 2014 (available at http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email); USA v. In Re: Information Associated with an Email Account at Lavabit.com, 1:13 EC297 (E.D. Va. 2013).

their products and services at the outset so that they can readily comply with law enforcement demands for user data, but remain exposed to malicious attacks and regulatory enforcement actions; or (2) build and maintain strong security, but incur the substantial costs of being compelled to weaken that security repeatedly to comply with law enforcement demands. Congress, which is accountable to the electorate, is better positioned to weigh the competing interests in play here and should be the branch that makes the policy decision whether, and to what extent, law enforcement's interests justify companies and their customers to bear those consequences, not this Court via an *ex parte* application under the All Writs Act.

3. The Burden the Government's Interpretation of the All Writs Act Would Impose on Businesses is Not Confined to Compliance With a Single Order.

The government argues that the Order is not a burden to Apple, because its request is confined to a single device and because the owner of the device in question—the shooter's employer—consented to the government's search. *See* Motion to Compel (Dkt. No. 1) at 17-18. These arguments are both straw men. As set forth above and in Apple's motion, designing new features to undermine the security of *one* device, necessarily undermines the security of *all* Apple devices, especially in light of the fact that the government has sought, and will almost certainly continue to seek, similar orders time and time again. Judge Orenstein succinctly dismantled the government's identical argument:

> The Application before this court is by no means singular: the government has to date successfully invoked the AWA to secure Apple's compelled assistance in bypassing the passcode security of Apple devices at least 70 times in the past; it has pending litigation in a dozen more cases in which Apple has not yet been forced to provide such assistance; and in its most recent use of the statute it goes so far as to contend that a court – without any legislative authority other than the AWA – can require Apple to create a brand new product that

> impairs the utility of the products it is in the business of selling. It is thus clear that the government is relying on the AWA as a source of authority that is legislative in every meaningful way: something that can be cited as a basis for getting the relief it seeks in case after case without any need for adjudication of the particular circumstances of an individual case . . . .

In re Order, 2016 WL 783565, at *15. And there is no reason to doubt that, if this Court adopts the government's expansive view of the All Writs Act here, the government will attempt to wield that authority beyond Apple.

II. CALEA LIMITS THE APPLICATION OF THE ALL WRITS ACT TO COMPEL ASSISTANCE IN BREAKING USER-CONTROLLED ENCRYPTION

Courts cannot use the All Writs Act to grant the government powers that Congress has considered and declined to give. The All Writs Act is a limited tool granting courts *ancillary* authority; it does not create new authority where none existed. *See Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 42 n.7 (1985) (the All Writs Act may be used "to fill statutory interstices."). As one court has observed, the All Writs Act is not "a mechanism for the judiciary to give [the government] the investigative tools that Congress has not." *In re Application of the United States for an Order Authorizing the Use of a Pen Register*, 396 F. Supp. 2d 294, 325 (E.D.N.Y. 2005). Where a court issues an order "that accomplishes something Congress has considered but declined to adopt – albeit without explicitly or implicitly prohibiting it" that order is not agreeable to the "usages and principles of law." *In re Order*, 2016 WL 783565, at *9.

Congress has already declined to grant law enforcement the power it seeks here. Through the legislative framework Congress has erected in the Communications Assistance for Law Enforcement Act (CALEA), P.L. 103-414, 47 U.S.C. § 1001, *et seq.* and the Stored Communications Act, Congress has never given law enforcement the authority to obtain what it seeks by way of court order

here. Therefore, as Judge Orenstein held, "what the government seeks here is to have the court give it authority that Congress chose not to confer." *In re Order*, 2016 WL 783565, at *16 (internal quotation and citation omitted). Under principles of separation of powers, the Court must decline to do so. *Id.* at *16.

A. CALEA Imposes Strict Limits on the Government's Ability to Compel Access to Encrypted Communications or to Command Particular Technology Designs.

When Congress enacted CALEA, it required a narrowly defined set of "telecommunications carrier[s]" to be able to assist law enforcement's ability to intercept voice and electronic communications upon a court order, subject to important limitations discussed below. 47 U.S.C. § 1001(8). In the original enactment, Congress defined telecommunications carriers to mean "common carrier[s]," principally telecommunications service providers connected to the publicly switched telephone network ("PSTN"), including wireline services and commercial mobile services. *Id.* Through its statutory rule-making authority, 47 U.S.C. § 1001(8)(B)(ii), the Federal Communications Commission later included broadband Internet service providers and Voice over IP phone services that connect to the PSTN in the definition of "telecommunications carriers."

Importantly, in the interest of not limiting technological advancement and innovation, Congress expressly *excluded* a separate class of Internet-based communications services, known as "information services," from the definition of "telecommunications carriers." 47 U.S.C. § 1001(8)(C)(i). An information service offers:

> a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and
>
> (B) includes—
>
> (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage

facilities;

(ii) electronic publishing; and

(iii) electronic messaging services

47 U.S.C. § 1001. This definition encompasses most of the Internet-based services used by both consumers and businesses for communication, productivity and entertainment, including cloud-based storage like Apple's iCloud service, social networks and chat messaging applications. *See In re Order.*, 2016 WL 783565, at *11 ("CALEA thus prescribes for telecommunications carriers certain obligations with respect to law enforcement investigations that it does not impose on a category of other entities—described as "information service providers"—that easily encompasses Apple.")

Congress further excluded information services from the obligations imposed by CALEA on telecommunications services to facilitate interceptions of their users' communications. 47 U.S.C. § 1002(b)(2)(a). These exclusions were the result of Congress' balancing the legitimate needs of law enforcement against privacy concerns that could inhibit the growth of the Internet economy. *See, e.g.*, H.R. Rep. No. 103-827, at 18 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3498 ("It is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed. . . . [E]xcluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line."). As Judge Orenstein concluded, "CALEA does not compel a private company such as Apple to provide the kind of assistance the government seeks here" does not constitute silence on the matter, but "reflects a legislative choice." *In re Order*, 2016 WL 783565, at *10.

Congress further balanced privacy and security interests with the law enforcement needs by including two key exceptions to the obligations of telecommunications companies to facilitate interceptions of user communications. First, the statute "*does not authorize* any law enforcement agency or officer" to

require a provider of wire or electronic communications services or any manufacturer of telecommunications equipment to adopt "any specific design of equipment, facilities, services, features, or system configurations." 47 U.S.C. § 1002(b)(1)(A) (emphasis added). Nor does it prohibit any such service or manufacturer from adopting any "equipment, facility, service, or feature." 47 U.S.C. § 1002(b)(1)(B). Second, Congress provided that a "telecommunications carrier 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) (emphasis added). Read together, Congress declared that electronic communications service providers and telecommunications equipment manufacturers may build strong, user-controlled encryption into their services, and that law enforcement cannot compel those providers to assist or ensure the government's ability to decrypt those communications.[15]

As Judge Orenstein recognized, CALEA does not exist in isolation. Congress has also legislated the procedures by which the government can compel providers of electronic communications services and remote computing services to produce the content of their subscribers' stored communications, when it enacted the Stored Communications Act, 18 U.S.C. § 2701, et seq. (the "SCA") in 1986 – eight years before it enacted CALEA. The SCA defines the types of user data the

[15] Congress decided that manufacturers of "telecommunications equipment" should have some CALEA compliance obligations, but that those obligations were limited by 47 U.S.C. § 1002(b)(1)(A). Congress also chose to *not* impose *any* burdens on other manufacturers of customer-owned devices that are not "telecommunications equipment." In particular, Congress consciously chose *not* to impose any regulation on or require assistance from manufacturers of end-user owned devices, which is why similar protection against forced decryption was not extended to them as part of the package of regulatory burdens and benefits applied to telecommunications service providers and telecommunications equipment manufacturers. *See* 47 U.S.C. §1005(b) and 1002(b)(2)(B).

government may access with a search warrant, court order or subpoena. *See* 18 U.S.C. § 2703. Although the law is not a model of clarity, one thing is clear: nothing in the statute requires providers of electronic communications and remote computing services to help the government decrypt encrypted communications. Nor does it prohibit providers from allowing their users to encrypt their data with user-controlled keys.

Congress could have drafted CALEA to require information services to assist law enforcement in complying with electronic intercept orders, but it chose to do the opposite. Congress could have drafted the statute to *prohibit* telecommunications carriers and information services from allowing end users to have exclusive control over decryption keys for communications on their respective networks, but it did not. To the contrary, Congress expressly *allowed* telecommunications carriers to offer their customers user-controlled encryption, without any obligation to assist the government's efforts to decrypt those communications. Congress similarly could have drafted CALEA's assistance requirements to apply to stored data, rather than only "data in motion," but it did not. Congress could have written or amended the SCA to require providers of electronic communications services and remote computing services to help the government decrypt users' communications, but it did not.[16] And in the 22 years following the enactment of CALEA, Congress has declined to abandon any of these restrictions, despite the country having faced a devastating terrorist attack, two wars, and the FBI's stated concerns to Congress about "going dark"—losing access to investigative information as a result of encryption. *See* U.S. Senate, Select Comm. on Intelligence, *Counterterrorism, Counterintelligence, and the Challenges of 'Going Dark.' July 8, 2015.* 114th Cong. (testimony of FBI Director James Comey). The Court should not do here what Congress has declined to do.

[16] Whether such provisions in CALEA or the SCA would have passed constitutional muster or would have been signed by the President are separate matters.

B. The Government's Attempt to Distinguish CALEA Would Create an Exception to CALEA That Would Swallow the Rule.

In its brief on its motion to compel Apple to comply with the Order (Dkt. No. 1), the government attempts to downplay the significance of CALEA, arguing that the relevance of the statute is limited to orders for "real-time interceptions and call-identifying information (data 'in-motion')" while this case involves "data 'at-rest.'" Motion to Compel at 22-23. But the government's logic fails. As discussed above, Congress *has* enacted legislation concerning government access to data "at rest" with electronic communications and remote computing services. *See* 18 U.S.C. § 2703. As Judge Orenstein pointed out, to focus on the "distinction between data 'at rest' and data 'in motion'" here "ultimately misses the point" because "[e]ven if Congress did not in any way regulate data 'at rest' in CALEA, it plainly could, and did, enact such legislation elsewhere." *In re Order*, 2016 WL 783565, at *11 (citing as an example 18 U.S.C. § 2703(f)(1)).

The government's analogy to *New York Telephone's* authorization of the use of the All Writs Act to compel a company to assist with the installation of a pen register is entirely backwards. There, Congress had enacted Title III, authorizing the use of wiretaps to intercept the content of communications, but had not yet enacted legislation expressly authorizing the real-time collection of less sensitive dialing information that is captured by a pen register. In finding that the order in that case was "not only consistent with the [All Writs] Act but also with more recent congressional actions," the Court reasoned that "it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy" than the interception of call content. *N.Y. Tel. Co.,* 434 U.S. at 177. The converse is true here. Compelling a company to help the government break a user's encrypted data—a power Congress expressly withheld from the government in

CALEA—is a far greater invasion of privacy than what Congress has authorized.

The government's expansive interpretation of the All Writs Act has dangerous implications. By its rationale, it could require companies that provide software for Internet-connected devices—also known as the "Internet of Things"—to create and cryptographically sign software "updates" to deploy to those devices to "assist" law enforcement's needs, whether by storing and periodically uploading data to law enforcement or by identifying a user's location. Or the government could force anti-malware vendors to ignore or even distribute malicious code, crippling the security the software is meant to provide, and irredeemably damaging trust in the vendor. Under the government's reading of the All Writs Act, this would be permissible, because the government would not be intercepting content "in motion." The potential impact to companies doing business in America could be substantial. Whether such an expansion of the government's surveillance powers is wise should be addressed by Congress, not the courts. *See In re Order*, 2016 WL 783565, at n. 26 ("[T]he government's theory that a licensing agreement allows it to compel the manufacturers of [Internet of Things] products to help it surveil the products' users will result in a virtually limitless expansion of the government's legal authority to surreptitiously intrude on personal privacy.").

III. THE *EX PARTE* NATURE OF THESE PROCEEDINGS IS IMPROPER AND IMPLICATES THE DUE PROCESS RIGHTS OF COMPANIES BEING COMPELLED UNDER THE ALL WRITS ACT.

Compounding the host of substantive issues with the government's application is the troubling process by which the Court issued its Order, which compelled Apple to comply without an opportunity to be heard. The government applied for and obtained the Order all in the course of one day. *See* Application; Order (both filed February 16, 2016). Apple received no notice and had no opportunity to be heard on the application prior to the Order issuing. Motion at 11, n. 22. But there was no need for the government to seek (nor for the Court to issue) an Order unprecedented in scope and nature using an *ex parte* procedure. This

approach raises serious concerns, both about due process and about the significant burden on third parties forced to respond quickly to such orders in the future.

Although the Court has now provided Apple an opportunity to be heard, that opportunity came only after the issuance of the Order, giving Apple only days to attempt to comply with or seek relief from the Order. In contrast, Judge Orenstein declined to rule *ex parte* on an even less burdensome application, finding Apple's input to be an "important missing piece of the analysis" and affording Apple the chance to respond to the application *prior* to ruling on the application. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, No. 15-mc-01902, 2015 WL 5920207, at *7 (E.D.N.Y. Oct. 9, 2015). Now, after benefitting from briefing and argument, Judge Orenstein has denied the government's motion. *In re Order*, 2016 WL 783565, at *1.

While, in exigent circumstances, a party must occasionally resort to *ex parte* proceedings, those situations are the exception, not the rule. *See United States v. Thompson*, 827 F.2d 1254, 1255 (9th Cir. 1987). Here, the government's desire to obtain information from the iPhone should not have trumped affording Apple the opportunity to be heard prior to a ruling. The phone's user was deceased, and in light of the widespread media attention given to the horrifying incidents of December 2, 2015, the government's investigation was not a secret. There was also no risk Apple would abscond with, destroy, or otherwise make unavailable the information the government seeks.

Further, because *ex parte* proceedings happen so quickly, they are likely to impose greater burdens on smaller companies that lack the resources to respond effectively to the demands such procedures entail, putting their rights at greater risk. While a company like Apple can marshal resources to oppose a demand with which it disagrees, even in an exceedingly difficult procedural posture, many smaller companies simply could not effectively fight such a demand. Faced with the risk of being held in contempt of court for non-compliance, those companies

might have no choice but to comply, regardless of principled objections. The government should not be allowed to abuse *ex parte* proceedings in this manner.

CONCLUSION

For these reasons, the Court should vacate its Order.

Dated: March 3, 2016

FENWICK & WEST LLP

By: _____
Tyler G. Newby

Andrew P. Bridges
David L. Hayes
Tyler G. Newby
Ciara N. Mittan
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile: 415.281.1350
abridges@fenwick.com
dhayes@fenwick.com
tnewby@fenwick.com
cmittan@fenwick.com

Attorneys for *Amici Curiae*