MAYER BROWN LLP
JOHN NADOLENCO (SBN 181128)
jnadolenco@mayerbrown.com
RUTH ZADIKANY (SBN 260288)
rzadikany@mayerbrown.com
350 South Grand Avenue, 25th Floor
Los Angeles, California 90071-1503
Telephone: (213) 229-9500
Facsimile: (213) 625-0248

ANDREW J. PINCUS (*pro hac vice application forthcoming*)
apincus@mayerbrown.com
TRAVIS CRUM (*pro hac vice application forthcoming)*
tcrum@mayerbrown.com
1999 K Street, N.W.
Washington D.C. 20006-1001
Telephone: (202) 263-3328
Facsimile: (202) 263-5328

Attorneys for *Amici Curiae* BSA|The Software Alliance, the Consumer Technology Association, the Information Technology Industry Council, and TechNet

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, EASTERN DIVISION

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

Case No. 5:16-cm-00010-SP

Brief of BSA|The Software Alliance, the Consumer Technology Association, the Information Technology Industry Council, and TechNet As *Amici Curiae* In Support Of Apple's Motion To Vacate And In Opposition To The Motion To Compel Assistance

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*

Amici are associations whose members comprise all of the companies that are leaders in the global technology industry. Because the Court's decision in this case could have significant effects on the security of the products created by *amici*'s members, and on the development of new hardware and software products, *amici* have a substantial interest in this proceeding.

BSA | The Software Alliance is an association of the world's leading software and hardware technology companies. BSA promotes policies that foster innovation, growth, and a competitive marketplace for commercial software and related technologies.

The Consumer Technology Association (CTA), formerly Consumer Electronics Association (CEA), is a trade association representing the $287 billion U.S. consumer electronics industry. CTA also owns and produces CES—the world's gathering place for all who thrive on the business of consumer technology.

The Information Technology Industry Council (ITI) is the global voice of the technology sector. As an advocacy and policy organization for the world's leading innovation companies, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world.

TechNet is an association of chief executive officers and senior executives of the Nation's leading technology companies across the country. TechNet's objective is to promote the growth of the technology industry and to advance America's global leadership in innovation. Its members are in the fields of information technology, biotechnology, clean technology, venture capital, e-commerce, and finance, and represent more than two million employees.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

This dispute between Apple and the United States arises in the context of a horrific crime that all Americans, and people around the world, condemn. The dispute implicates a number of vitally important policy interests:

- Law enforcement and protection of Americans against terrorism;
- Individuals' right to keep secure against hackers and other bad actors their most personal information and communications;
- The scope of the government's power to force a private party to act as an agent of the government; and
- The extent to which the government may, and should, prescribe product design requirements for technology products.

FBI Director James Comey was not engaging in hyperbole when he described harmonizing these vital interests as "the hardest question I've seen in government," requiring consideration of "who do we want to be as a country, and how do we want to govern ourselves." Zadikany Decl. Ex. A [Brian Bennett, *FBI Director Calls Apple Case 'Hardest Question' In Government*, L.A. Times (Feb. 25, 2016)].

The All Writs Act does not give this Court the power to reconcile these fundamental policy issues. When Congress enacted that statute in 1789 it neither anticipated nor broadly authorized government conscription of private parties that might be able to assist a government investigation—which is the essence of the government's position.

Moreover, the government's interpretation of the statute effectively limits this Court's inquiry to law enforcement needs and dollars-and-cents economic burden, and leaves no room for consideration of the other important interests at stake—such as maintaining security of individuals' most personal information, risk to a third party's business and reputation, potential damage to development of new technology that would result from government-mandated design specifications, and

whether in our constitutional democracy specific congressional authorization should be required before courts may determine on an ad hoc basis that a private individual or company should be forced to assist in government investigations. The Court accordingly should vacate the order on the ground that it exceeds the authority conferred by the All Writs Act.

Controlling circuit precedent confirms that a company cannot be compelled to develop a new product—here, new software that does not now exist—particularly when it will create security risks for all users of the company's products. The government's argument, moreover, has no limiting principle: any third party could be conscripted to produce new software that would allow the government to breach security measures. Congress could not have intended that result when it enacted the All Writs Act in 1789—indeed, when Congress has authorized conscription of unwilling private parties it has spoken clearly, and provided specific standards to govern the imposition of such obligations. Finally, the predictable result of upholding the government's position will be to force companies to change the design specifications they might otherwise utilize in response to the risk that they might be subject to an order such as the one sought here. A decision with such significant public policy consequences should be made by the People acting through the political branches—not through the issuance of an order by this Court.

ARGUMENT

A Court May Invoke The All Writs Act To Compel A Third Party To Turn Over Or Provide Access To Existing Information The Third Party Possesses, But May Not Order A Third Party To Invent A New Product—Particularly When The Government's Demand Would Create Security Risks And Effectively Dictate Product Design.

The general language of the All Writs Act "is not a grant of plenary power to federal courts." *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir.

1979).[1] In the context here—requiring a third party to assist in a government investigation—the Act has been invoked in three basic situations:

- Requiring the third party to turn over information in its possession that the government has a lawful right to obtain. *See, e.g.*, *United States v. Hall*, 583 F. Supp. 717 (E.D. Va. 1984) (compelling credit card company to turn over records in its possession); *In re Application of United States for an Order Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003) (unpublished) (directing landlord to turn over security footage in its possession).
- Compelling the third party to turn over a password possessed by the third party that is needed to obtain access to information covered by the underlying warrant or other legal process.
- When the information that the government has a legal right to obtain is possessed by the third party as a result of a government-conferred monopoly, obligating the third party to enable the government to obtain access to that information. *United States v. New York Telephone Co.*, 434 U.S. 159 (1977); *In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities*, 616 F.2d 1122 (9th Cir. 1980).

All of the cases cited by the government that involve process directed at third parties, other than two recent ruling involving the factual situation presented here, fall into these categories.

The government's request here is dramatically different in kind. The government has possession of the device containing the information at issue. Apple

---

[1] The Act provides: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a).

does not have the password that would unlock the device. The government instead would require Apple to create a new product, a new software "tool," meeting the list of requirements specified by the government. That demand bears no resemblance to the three situations in which process has previously been authorized under the All Writs Act.

The government cites two district court decisions—one issued *ex parte* and one without any analysis—that endorse its position.[2] Another court recently rejected the government's position in a lengthy opinion. *See In re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court*, No. 15 MC 1902 (E.D.N.Y. Feb. 29, 2016), Doc. 29.

This Court should hold that the government's request falls outside the authority conferred by the All Writs Act.

A. Precedent Prohibits The Order Sought By The Government.

The government is unable to point to a single authoritative precedent in support of its extraordinarily expansive construction of the Act. Its argument must be rejected for two reasons. First, the Act simply does not reach beyond the three situations in which it has routinely been applied. Second, even if the Act *could* extend more broadly, it cannot apply in the circumstances presented here.

1. The Ninth Circuit's rejection in *Plum Creek* of a similarly unprecedented application of the All Writs Act demonstrates the flaws in the government's analysis here.

That case arose in the context of an investigation by the Occupational Safety and Health Administration (OSHA) of a lumber yard explosion. During its investigation, OSHA requested that the lumber yard's employees wear noise-

[2] *See* Apple Mem. in Support of Motion to Vacate at 28 (discussing *United States v. Navarro*, No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013), ECF No. 39; *In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone*, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014).

measuring devices and air containment sampling devices. The company had a policy barring its employees from wearing such devices, claiming, in relevant part, that the devices were "dangerous because they could distract employees or cause them to become entangled in moving equipment." 608 F.2d at 1286. OSHA sought an order pursuant to the All Writs Act compelling the company to allow its employees to wear the devices.

The Ninth Circuit held that the Act did not authorize OSHA's proposed order—even though the lumber company was the target of the investigation. The Court relied on a number of factors in concluding that

> although the use of the personal noise-level and air-contaminant measuring devices is a reasonable means of inspecting, there is no statutory or inherent authority in the district court to order Plum Creek to rescind its policy forbidding its employees to wear the OSHA devices.

608 F.2d at 1290. The Ninth Circuit held that the All Writs Act "does not authorize a court to order a party to bear risks not otherwise demanded by law." *Id.* at 1289-1290.[3]

The Ninth Circuit thus refused to impose upon a private party a duty not otherwise required by law—a duty that required the creation of information, rather than merely providing the government with existing information in the possession of the private party. The court of appeals' reasoning requires rejection of the government's request here. *Cf. New York Telephone*, 434 U.S. at 174 (concluding that, because telephone monopoly's own facilities were "being employed to facilitate a criminal enterprise on a continuing basis," the company was not "so far removed from the underlying controversy that its assistance could not permissibly

---

[3] The Ninth Circuit also noted that OSHA had less-effective alternative means of conducting its investigation of Plum Creek, but it did not state that the result would have been different if those alternatives did not exist. *See Plum Creek Lumber Co.*, 608 F.2d at 1289.

be compelled").

The court of appeals' conclusion about the limited scope of the All Writs Act makes sense for an additional reason: a contrary result would embroil the courts in wholly unguided assessments of the consequences to a third party of compelling it to perform the tasks demanded by the government. Different courts could reach different conclusions on that question, but those different results could have very significant consequences for the security of data held by those companies—which would be particularly unfair if, as is likely, the companies were marketplace competitors.

Moreover, such ad hoc determinations would leave businesses and other private parties with no certainty about their potential legal obligations. Businesses would be unable to anticipate government demands that might be asserted, or how such demands would be resolved by the courts.

2. Even if the Act could in some circumstances extend beyond situations in which the government seeks disclosure of or access to existing information in the possession of a third party, an order would be impermissible here.

Courts have limited the conscription of third parties under the Act to situations in which the government's demand would not subject the third party to an unreasonable burden. *New York Telephone Co.*, 434 U.S. at 172 ("[U]nreasonable burdens may not be imposed."); *id.* at 175 ("Nor was the District Court's order in any way burdensome. The order provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the Company and no disruption to its operations."); *Plum Creek Lumber Co.*, 608 F.2d at 1289-90 ("[The All Writs Act] does not authorize a court to order a party to bear risks not otherwise demanded by law.").

The order here would impose very substantial burdens and risks on Apple and its customers.

First, the government's order would create a very real security risk for the

millions of Apple products with the same operating system as the iPhone involved here. That imposes a substantial burden on Apple's customers and on Apple.

The Supreme Court recently explained in detail the intensely personal nature of the information contained on these devices:

> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. *The sum of an individual's private life can be reconstructed* through a thousand photographs labeled with dates, locations, and descriptions . . . . Third, the data on a phone can date back to the purchase of the phone, or even earlier. . . . Finally, there is an element of pervasiveness that characterizes [information contained in] cell phones.

Riley v. California, 134 S. Ct. 2473, 2489-90 (2014) (emphasis added).

Apparently recognizing the deeply private nature of the data contained on these devices, and the security risks inherent in circumventing encryption software, the government argues that there is no danger here because the software that Apple would be compelled to create would be used only for this one phone—and could be retained in Apple's possession and then destroyed. That is an unrealistic picture of the consequences of upholding the government's demand.

To begin with, the government itself has made clear that this is not a one-off request. The Department of Justice has asserted multiple demands for the creation of this software, and other law enforcement officials have indicated that they too would utilize the Act or state equivalents to impose the same obligation. *See* Apple Mem. In Support of Motion to Vacate at 3. It would hardly make sense for a company faced with multiple demands to continuously create and destroy the software.

Once software is created to circumvent the device's security protections—both the password-protection feature and the "auto erase" function after ten incorrect entries—that software could fall into the wrong hands: it could be stolen by hackers or by a government intelligence agency. *See* Apple Mem. In Support of Motion to Vacate at 5-8.

Moreover, there is a significant risk that multiple uses of such government-specified software will inevitably lead to public disclosure of information that would enable hackers (whether private or sponsored by foreign governments) to produce their own hacking tool. If, for example, the software resulted in access to evidence that federal or state authorities sought to introduce in a criminal proceeding, the Apple engineers who created the government-mandated software could be required to testify about how the software tool worked and to provide assurance that it merely provided access to, and did not in any way alter, the information contained on the device in question. That testimony, in turn, could provide hackers with a roadmap to create their own tool for invading the contents of the device. *Cf.* Apple Mem. In Support of Motion to Vacate 24-25. The only effective way to prevent this software from falling into the wrongs hands is to abstain from creating it in the first place.

In sum, the significant security risks to all device users that would result from creation of the software demanded by the government is an unreasonable burden under the *New York Telephone* standard that bars issuance of the order.

Second, the government's order would force a company to breach its assurances to its customers about the security of their information, possibly subjecting it to liability as well as harm in the marketplace.

Customers are intensely concerned about maintaining control over their most intimate and personal information. "[P]eople now are more anxious about the security of their personal data and are more aware that greater and greater volumes of data are being collected about them." Zadikany Decl. Ex. B [Lee Rainie & Shiva

Maniam, *Americans Feel the Tensions between Privacy and Security Concerns*, Pew Research Center (Feb. 19, 2016)]. Eighty percent of adults "agree" or "strongly agree" that Americans should be concerned about the government's monitoring of phone calls and internet communications. Zadikany Decl. Ex. C [Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 12, 2014)].

These concerns have been heightened by the revelations by Edward Snowden about U.S. government access to personal information. Consumers are also very sensitive to and concerned by the threats to security of their private information posed by an array of criminals and bad actors, including hackers, fraudsters, and identity thieves. *See* Zadikany Decl. Ex. D [Rebecca Riffkin, *Hacking Tops List of Crimes Americans Worry About Most*, Gallup (Oct. 27, 2014)].

Many technology companies have announced changes to their operating systems specifically designed to provide customers with greater security for their personal information. *See, e.g.*, Hanna Decl. Ex. M [Berkman Center for Internet & Society at Harvard University, *Don't Panic: Making Progress on the "Going Dark" Debate*, at 3-4 (2016)].

The order sought by the government would force Apple to undermine the hard-earned trust of its customers. That will subject the company to substantial reputational and marketplace injury, leading customers to lose confidence in the company's willingness to protect their security and seek trustworthy alternatives that provide greater protection.

These harms could be particularly pronounced in other nations where protection of personal information in general, and distrust of the U.S. government in particular, is highly relevant in the marketplace. Indeed, some U.S. technology companies suffered substantial economic and reputational harm in the wake of the revelations about U.S. government access to personal information. *See* Zadikany

Decl. Ex. E [Gerry Smith, *'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions*, Huffington Post (Jan. 24, 2014)] (noting that in the wake of Snowden's revelations, approximately ten percent of non-U.S. companies cancelled contracts with U.S. companies out of fear of NSA surveillance).

Foreign competitors in particular would argue that devices or software created by U.S. companies are less secure because of the risk that the U.S. government would demand creation of a "tool" to enable access to personal information—and that customers should therefore purchase only from non-U.S. technology companies. This is not speculation: these very arguments were advanced in the wake of the Snowden revelations. *See* Zadikany Decl. Ex. F [Charles Babcock, *NSA's Prism Could Cost U.S. Cloud Companies $45 Billion*, InformationWeek (Aug. 14, 2013)] (Neelie Kroes—at the time, the European Commissioner for Digital Affairs—observed: "If European cloud customers cannot trust the United States government, then maybe they won't trust U.S. cloud providers either. . . . If I were an American cloud provider, I would be quite frustrated with my government right now.").

If Congress wants to subject American businesses to these burdens, it can do so explicitly; but this Court should not interpret the All Writs Act implicitly to authorize courts to inflict such consequences based on ad hoc decisions without any guidance from Congress.

Third, foreign nations, including repressive regimes, would argue that they, too, may compel Apple—and other companies—to use their technical expertise to access locked phones and other devices, including those seized from political and religious dissidents or journalists. Companies that refuse assistance might well be told: the United States government compels this assistance, we may do so as well. And these foreign governments could refuse to impose the same safeguards the U.S. government proposes in this case, thereby making it far more likely that repressive regimes could use unrestricted access to cellphones' content to

persecute their own citizens for exercising free speech and similar human rights.

* * * * *

In *Plum Creek*, the Ninth Circuit held that the government's request fell outside the All Writs Act because the order would subject the lumber company to risk. It observed that as a "private employer," the company "bears all safety risks. The safety factor cannot be eliminated. [The employer] pays the cost of all industrial accidents. OSHA cannot guarantee that these devices would cause none." *Id.* at 1289. The court of appeals held that "in the absence of law specifying [the devices] use, we cannot order [the employer] to bear the added risks the devices would bring." *Id.*

The Department of Justice here, like OSHA in *Plum Creek*, cannot guarantee that the foreseeable security risks—borne by Apple's customers and Apple itself—will not be realized. Just as the All Writs Act did not give "court[s] a roving commission to order a party subject to an investigation to accept additional risks at the bidding of OSHA inspectors," *id.*, the Act also does not authorize the government to force Apple to create a massive security vulnerability for its devices, causing serious and potentially irreparable economic and reputational harm to the company, as well as potentially infringing the fundamental human rights of individuals using its products around the world.

B. The Government's Expansive Interpretation Of The Act Has No Limiting Principle.

The order should be vacated for the additional reason that it rests on a construction of the All Writs Act that has no limiting principle. Under the government's approach, any private party may be forced against its will to assist the government in any way, subject only to the vague "unreasonable burden" limitation. Courts would be obliged to apply this standard on an ad hoc basis in numerous cases—involving different devices, device manufacturers, and software creators—that inevitably will follow this one if the government is successful. The

Court should refuse to interpret the statute to produce such a substantial intrusion on liberty in the absence of express congressional authorization.

The target of the government's request in this case is Apple, but the government's theory would just as easily extend to any third-party developer of software that has as one of its functions collecting and storing personal information about the device's owner. All such software includes security measures to protect the owner's personal information—and the government's theory would empower it to require the software creator to develop a "tool" to enable the government to access that information. The authority sought by the government would therefore extend not only to phones, laptop computers, and tablets, but also to automobiles that store information regarding location and times of use; insulin pumps that store information about blood sugar levels; and the myriad other devices that collect and store personal information.

Creation of government-required software tools providing access to the information stored on any such device would multiply the security risks and other burdens described above. These burdens would fall most heavily on smaller, younger technology companies—such as start-ups—that will have fewer employees and less resources.

The government's decisions regarding which companies to target—and courts' case-specific decisions regarding which government requests could grant—could have significant marketplace consequences. Companies forced to invent new tools to facilitate government access would have to take on risks and could be disadvantaged in the marketplace vis-à-vis competitors not forced to do so. And the uncertainty over the scope of the government's authority itself would impose significant costs on all businesses.

Importantly, although the government focuses on the horrific nature of the underlying crime here, nothing in the government's interpretation of the statute would limit such orders to crimes of great magnitude. Indeed, as discussed above

(*see* page 8, *supra*), the federal government and state and local prosecutors have already made clear that they believe their interpretation extends broadly to any criminal investigation.[4]

The government's theory, moreover, is not limited to digital technology. What if the government were unable to break into an "unbreakable" safe? Could the government force the company that made the safe to design a way to defeat its own product? Or suppose the government seized encoded records. Could the government conscript MIT graduate students to break the code?

The government can of course employ its own resources—its own employees and its own funds—to accomplish the ends it desires. But the All Writs Act does not confer a broad license upon the government to force unwilling private companies and individuals to accede to its demands.[5]

---

[4] In addition, nothing in the All Writs Act limits the statute's scope to criminal cases. It is not inconceivable that private plaintiffs will argue that they may invoke the All Writs Act in the same manner that the government attempts here, but in furtherance of civil discovery orders.

[5] An expert on cybersecurity issues, testifying before the House Judiciary Committee, urged Congress to address this issue by giving the FBI the resources needed to "[b]ring FBI investigative capacity into the twenty-first century":

> The Bureau has some expertise in this direction, but it will need more, much more, both in numbers and in depth. The FBI will need an investigative center with agents with a deep technical understanding of modern telecommunications technologies; this means from the physical layer to the virtual one, and all the pieces in between. Since all phones are computers these days, this center will need to have the same level of deep expertise in computer science. In addition, there will need to be teams of researchers who understand various types of fielded devices. This will include not only where technology is and will be in six months, but where it may be in two to five years. This center will need to conduct research as to what new surveillance technologies will

(cont'd)

C. When Congress Intends To Authorize Government Conscription Of Private Parties, It Does So Expressly.

The absence from the All Writs Act of any express authority for conscripting third parties provides another reason for rejecting the government's request. Congress in other contexts has acted clearly and expressly when authorizing the federal government to force private parties to do the government's bidding.

For example, the Defense Production Act, 50 U.S.C. § 4501 *et seq.*, confers authority on the President to require private persons or companies to accept contracts necessary for the national defense. *Id.* § 4511. That authority is explicit, specific, and subject to a variety of restrictions, including narrow definitions of when the statute may be invoked, *see id.* § 4552. The Defense Production Act also has provisions requiring specific congressional authorization, *see id.* § 4514(a) (wage and price controls), as well as a sunset provision, *see id.* § 4564.

Similarly, the Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001 *et seq.*, establishes a detailed statutory scheme governing the assistance that telecommunications providers are obligated to provide to the government. And CALEA expressly distinguishes between

---

(… cont'd)

> need to be developed as a result of the directions of new technologies. I am talking deep expertise here and strong capabilities, not light.
>
> This expertise need not be in house. The FBI could pursue a solution in which they develop some of their own expertise and closely manage contractors to do some of the work. But however the Bureau pursues a solution, it must develop modern, state-of-the-art capabilities for surveillance.

Zadikany Decl. Ex. G [Susan Landau, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, Hearing before the House Judiciary Comm. (Mar. 1, 2016)].

"telecommunications carriers" and "information services" providers, requiring only the former to enable the government to intercept communications pursuant to a court order. *Id.* §§ 1001(8), 1002. Apple plainly is not a "telecommunications carrier." Thus, when Congress enacted CALEA in 1994, it made a considered judgment to exclude information services providers such as Apple from the statute's obligations.

Indeed, Congress in 2015 held hearings on whether CALEA should be amended to require technology companies like Apple to assist law enforcement's requests for decryption. *See* Hanna Decl. Ex. L [Sally Quillian Yates and James B. Comey, Jr., *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption*, Hearing before the Senate Judiciary Comm. (July 8, 2015)].

The Executive Branch publicly decided not to seek legislation, however. *See* Hanna Decl. Ex. S [James B. Comey, *Statement Before the Senate Comm. On Homeland Sec. & Governmental Affairs*, Hearing Before the Senate Comm. On Homeland Sec. & Governmental Affairs (Oct. 8, 2015)]. And the Chairman of the Senate Judiciary Committee has criticized the Administration for failing to give Congress the information it needs to consider these important policy questions. Zadikany Decl. Ex. H [Letter from Sen. Charles E. Grassley to Sally Q. Yates, Deputy Att'y Gen., and James B. Comey, Jr., Dir., Fed. Bureau of Investigation, (Feb. 16, 2016)].

This Court should not transform the general language of the All Writs Act into all-purpose authority for compelling the very sorts of assistance from private companies that Congress has required only pursuant to detailed laws that carefully balance all of the relevant interests. To hold otherwise would violate the Supreme Court's instruction that the All Writs Act is designed only to "fill statutory interstices." *Pennsylvania Bur. of Corr. v. U.S. Marshals*, 474 U.S. 34, 42 n.7 (1985). It would confer upon the courts plenary, unguided authority to resolve a

policy issue so complex that the FBI Director has characterized it as the "hardest question" he has ever seen in government. And it would be inconsistent with the Supreme Court's ruling in the *Steel Seizure Cases* rejecting the federal government's analogous argument that the general language of the Constitution somehow authorized the President to seize and operate steel mills. *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

D. The Likely Practical Result of The Government's Position Will Be De Facto Government-Mandated Design Specifications.

Congress has explicitly refused to subject technology companies to government-imposed design specifications. CALEA expressly prohibits the government from requiring any "provider of . . . electronic communication service" to adopt a "specific design of equipment, facilities, services, features, or systems configuration." *Id.* §1002(b)(1). Granting the order sought here—and the large numbers of requests that are sure to follow in its wake—will have the practical effect of doing just that, circumventing Congress's intent in passing CALEA.

If Apple is compelled to develop the new software that the government demands, it is inevitable that the federal government, and state and local law enforcement, will seek to impose the same obligation on creators of other operating systems. Companies will then face a choice: continue to be burdened by such government demands, and design products in a manner that such demands can be more easily satisfied; or configure new versions of their operating systems to make development of such software "tools" impossible.

The first option would mean products intentionally designed to be less secure. That would not only subject customers to a greater risk of privacy intrusions, but also harm long-term U.S. economic interests and national security. *See, e.g.,* Hanna Decl. Ex. O [McConnell et al., *Why The Fear Over Ubiquitous Data Encryption Is Overblown,* Wash. Post (July 28, 2015)]. It would leave

ordinary citizens less secure, while malevolent actors would retain the ability to purchase completely-secure devices.

The second option—encouraging companies to configure products in a way that makes orders such as the one sought here impossible to implement—could have the result of making it even more difficult for law enforcement and national security agencies to access information. Indeed, it has been reported that Apple is already working on encryption software that would not be susceptible to the work-around sought by the government in this case. *See* Zadikany Decl. Ex. I [Matt Apuzzo & Katie Benner, *Apple Is Said To Be Trying To Make It Harder To Hack iPhone*, N.Y. Times (Feb. 24, 2016)]. The Court should not fuel that self-defeating result.

* * * * *

As Justice Alito has explained: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment). The All Writs Act plainly does not address this complex question. This Court should therefore reject the government's request, and leave resolution of these complex questions to policymakers.

CONCLUSION

The motion to vacate should be granted and the motion to compel assistance should be denied.

Dated: March 3, 2016

MAYER BROWN LLP
JOHN NADOLENCO
RUTH ZADIKANY
ANDREW J. PINCUS
TRAVIS CRUM

By: John Nadolenco per rz
John Nadolenco
Attorneys for *Amici Curiae* BSA|The Software Alliance, the Consumer Technology Association, the Information Technology Industry Council, and TechNet

PROOF OF SERVICE

I, Janice Austgen, declare:

I am employed in Los Angeles County, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is Mayer Brown LLP, 350 South Grand Avenue, 25th Floor, Los Angeles, California 90071-1503. On March 3, 2016, I served a copy of the within document(s):

BRIEF OF *AMICI CURIAE* BSA|THE SOFTWARE ALLIANCE, THE CONSUMER TECHNOLOGY ASSOCIATION, THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL, AND TECHNET

X by placing the document(s) listed above in a sealed UPS envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to a UPS agent for delivery.

SEE ATTACHED SERVICE LIST

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

Executed on March 3, 2016, at Los Angeles, California.

Janice Austgen

Eric David Vandevelde, Esq.
Theodore J. Boutrous, Jr., Esq.
Gibson Dunn and Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071

Jeffrey G. Landis, Esq.
Marc J Zwillinger, Esq.
Zwillgen PLLC
1900 M Street NW Suite 250
Washington, DC 20036

Nicola T. Hanna, Esq.
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 92612-4412

Theodore B. Olson, Esq.
Gibson Dunn and Crutcher LLP
1050 Connecticut Avenue NW
Washington, DC 20036-5306

Allen W. Chiu, Esq.
Assistant United States Attorney
Office of U.S. Attorney
National Security Section
312 North Spring Street Suite 1300
Los Angeles, CA 90012

Tracy L. Wilkison, Esq.
Assistant United States Attorney
Office of U.S. Attorney
Chief, Cyber and Intellectual Property Crimes Section
312 North Spring Street 11th Floor
Los Angeles, CA 90012-4700