JEROME C. ROTH (State Bar No. 159483)
jerome.roth@mto.com
ROSEMARIE T. RING (State Bar No. 220769)
rose.ring@mto.com
JONATHAN H. BLAVIN (State Bar No. 230269)
jonathan.blavin@mto.com
JOSHUA PATASHNIK (State Bar No. 295120)
josh.patashnik@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street
Twenty-Seventh Floor
San Francisco, California 94105-2907
Telephone: (415) 512-4000
Facsimile: (415) 512-4077

ARIEL C. GREEN (State Bar No. 304780)
ariel.green@mto.com
MUNGER, TOLLES & OLSON LLP
355 South Grand Avenue
Thirty-Fifth Floor
Los Angeles, California 90071-1560
Telephone: (213) 683-9100
Facsimile: (213) 687-7302

Attorneys for *Amici Curiae*

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. ED CM 16-10-SP **BRIEF OF *AMICI CURIAE* AIRBNB, INC.; ATLASSIAN PTY. LTD.; AUTOMATTIC INC.; CLOUDFLARE, INC.; EBAY INC.; GITHUB, INC.; KICKSTARTER, PBC; LINKEDIN CORPORATION; MAPBOX INC.; A MEDIUM CORPORATION; MEETUP, INC.; REDDIT, INC.; SQUARE, INC.; SQUARESPACE, INC.; TWILIO INC.; TWITTER, INC.; AND WICKR INC.** Judge: Hon. Sheri Pym

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

FEDERAL CASES

FEDERAL STATUTES

FEDERAL RULES

FEDERAL LEGISLATIVE MATERIALS

OTHER AUTHORITIES

I. INTEREST OF *AMICI CURIAE*

Amici curiae are providers of platforms and tools for communicating, publishing, connecting, transacting, and securing traffic over the Internet: Airbnb, Inc. ("Airbnb"), Atlassian Pty. Ltd. ("Atlassian"), Automattic Inc. ("Automattic"), CloudFlare, Inc. ("CloudFlare"), eBay Inc. ("eBay"), GitHub, Inc. ("GitHub"), Kickstarter, PBC ("Kickstarter"), LinkedIn Corporation ("LinkedIn"), Mapbox Inc. ("Mapbox"), A Medium Corporation ("Medium"), Meetup, Inc. ("Meetup"), Reddit, Inc. ("Reddit"), Square, Inc. ("Square"), Squarespace, Inc. ("Squarespace"), Twilio Inc. ("Twilio"), Twitter, Inc. ("Twitter"), and Wickr Inc. ("Wickr"). The number of users of their platforms and tools is over one billion.

Airbnb provides an Internet platform through which persons desiring to book accommodations, and persons listing unique accommodations available for rental, can locate each other and enter into direct agreements with each other to reserve and book travel accommodations on a short and long-term basis.

Atlassian's products help teams organize, discuss, and complete their work in a coordinated, efficient and modern fashion. Organizations use Atlassian's project tracking, content creation and sharing and real-time communication and service management products to work better together and deliver quality results on time.

Automattic is the company behind WordPress.com, the online publishing platform that serves more than 15.8 billion pages a month, as well as a host of other popular online services, such as WooCommerce, Jetpack, and Simplenote.

CloudFlare offers some of the most advanced web security, distributed denial of service attack mitigation, and content delivery solutions available. CloudFlare is a community of over 2 million websites handling as much as 5 percent of global web and blocking more than 8.3 billion potentially malicious requests every day.

eBay is a global commerce leader. With more than 160 million active buyers and more than 800 million live listings globally, eBay enables sellers worldwide to organize and offer their inventory for sale and buyers to find and buy virtually

anything, anytime, anywhere.

GitHub is a web-based hosting and collaboration platform where people discover, share and contribute to software.

Kickstarter is a worldwide community of people dedicated to bringing creative projects to life—a place where people come together to make new things like films, food trucks, board games, and innovative technology.

LinkedIn is an Internet company that hosts the world's largest professional network, with over 400 million members worldwide and over 122 million members in the United States. LinkedIn's mission is to connect the world's professionals to enable them to be more productive and successful.

Mapbox provides highly customizable maps and mapping software for web, mobile, and embedded applications. Based in Washington, D.C., Mapbox powers the maps behind some of the most visited sites on the web.

Medium, based in San Francisco, is an online publishing platform that allows anyone to easily read, write, and share stories and ideas that matter to them. Tens of millions of users have spent more than 3.5 millennia reading together on Medium.

Meetup is the world's largest network of local community groups, enabling people to connect with others online and engage in activities offline.

Reddit operates the reddit.com platform, which is a collection of thousands of online communities attracting over 230 million monthly unique visitors that create, read, join, discuss and vote on conversations across a myriad of topics.

Square creates tools and services to make commerce easy, from empowering sellers with the tools needed to take their first credit card payment, to providing software for every part of starting, running, and growing a business.

Squarespace provides web publishing and development platforms, including Squarespace.com, for creating high quality websites easily and affordably.

Twilio is a cloud communications platform that makes communications easy and powerful. With Twilio's platform, businesses can make communications relevant

and contextual by embedding real-time communication and authentication capabilities directly into their software applications.

Twitter is a global platform for public self-expression and conversation that gives users the power to create and share ideas, information, and rich media content with each other, instantly. Twitter has more than 300 million monthly active users who share hundreds of millions of Tweets per day.

Wickr is a secure communications platform which provides end-to-end encryption and industry-leading security to businesses and individuals around the world to safeguard high-value proprietary and personal data and communications.

As providers of several of the most popular communication, networking, ecommerce, publishing, and commercial transaction platforms on the Internet accessed via websites and/or applications on mobile devices, *Amici* have a strong interest in this case, the continued security and privacy of their users' data, and in transparency to users regarding how that data is protected. Several *Amici* also regularly assist in law-enforcement investigations and have a strong interest in ensuring that government requests for user data are made within the bounds of applicable laws, including those that balance the interests of privacy, security, and transparency with law enforcement needs.

II. SUMMARY OF ARGUMENT

The government in this case has invoked a centuries-old statute, the All Writs Act (the "Act"), to force Apple, Inc. ("Apple") to develop software to undermine its own carefully constructed security measures, which were designed to protect its customers' data from hacking, misuse, and theft. This extraordinary and unprecedented effort to compel a private company to become the government's investigative arm not only has no legal basis under the All Writs Act or any other law, but threatens the core principles of privacy, security, and transparency that underlie the fabric of the Internet.

In today's era of rapid technological change, these bedrock principles are more

vital than ever. The increasing ubiquity of the Internet in all aspects of life has ushered in a new generation of innovative products and services for consumers and businesses. In the midst of this digital revolution—and the ever-present and increasing dangers posed by hackers, identity thieves, and other wrongdoers—ensuring that users' data is handled in a safe, secure, and transparent manner that protects privacy is of utmost importance.

At the same time, *Amici* recognize and respect the government's important work in law enforcement and national security. Indeed, although *Amici* oppose any forced "backdoors" providing the government access to their systems, they do and will continue to comply with proper and reasonable requests for data pursuant to legal processes enacted by legislatures and consistent with the Constitution. But the government's efforts in this case—to force a private company to affirmatively develop software that does not currently exist in order to break its own security systems—would erode the privacy and protection of user data, and transparency as to how such data may be used or shared.

The government's demand here, at its core, is unbound by any legal limits. It would set a dangerous precedent, in which the government could sidestep established legal procedures authorized by thorough, nuanced statutes to obtain users' data in ways not contemplated by lawmakers. These laws include the federal Wiretap Act ("Title III") (codified at 18 U.S.C. §§ 2510, *et seq.*), the Stored Communications Act ("SCA") (codified at 18 U.S.C. §§ 2701, *et seq.*), the Communications Assistance for Law Enforcement Act ("CALEA") (codified at 47 U.S.C. §§ 1001, *et seq.*), and the Foreign Intelligence Surveillance Act ("FISA") (codified at 50 U.S.C. §§ 1801, *et seq.*). Together these statutes provide a comprehensive regulatory scheme enabling law-enforcement agencies to secure the assistance of third parties in accessing communications and data in connection with their investigative functions in the manner and subject to the limitations that Congress has deemed appropriate.

In enacting such laws, Congress balanced law enforcement and national

security needs with the important interests of protecting users' privacy and security. Congress also considered the impact that regulating or mandating certain levels of law-enforcement assistance may have on innovation, creativity and growth by the technology industry. By circumventing the procedures adopted by Congress, and thereby overturning the careful weighing of policy considerations they reflect, the government is seeking to enlist the judiciary in re-writing laws without engaging in an essential public debate. While *Amici* are sensitive to the emotionally charged atmosphere that can surround investigations such as this one, a meaningful discourse on this topic is critical for all members of our society as we strive to meet the challenge of finding the proper balance between privacy and liberty interests and the dangers posed by criminal and national-security threats.

The All Writs Act does not authorize the government to make an end-run around this important public debate and our nation's legislative processes. The Act is a gap-filling procedural measure, not a broad independent grant of substantive power to federal courts. Its purpose, dating back to the Judiciary Act of 1789, is to allow courts to issue writs necessary to effectuate their *existing* powers, not to give courts new powers. For that reason, the Supreme Court repeatedly has recognized that where another statute speaks to the issue at hand, the All Writs Act is displaced and the applicable statutory scheme governs. The government may not use the Act here to circumvent the limitations imposed by the existing, comprehensive statutory scheme to arrogate to itself powers that Congress has chosen not to provide it.

For these reasons and those discussed below, *Amici* respectfully urge the Court to deny the government's Motion to Compel and to grant Apple's Motion to Vacate.

III. ALLOWING THE GOVERNMENT TO FORCE COMPANIES TO UNDERMINE THEIR OWN PROMISED SECURITY MEASURES WILL ERODE THE CORE VALUES OF PRIVACY, SECURITY, AND TRANSPARENCY

The government's efforts in this case to force a private company to become its investigative arm and to take affirmative steps to undermine the company's own

promised security measures—essential to the protection of its users' data—are not only legally unprecedented and unfounded (as discussed below), but they will also erode the critically important principles of privacy, security, and transparency, causing tangible harm to users, Apple and the industry, and society more generally.

A. In The Current Era of Rapid Technological Change, the Core Values of Privacy, Security, and Transparency Are More Vital than Ever

In an era where technologies and business models are evolving as rapidly as they are now, the bedrock principles of privacy, security, and transparency are more important than ever.

An ever growing range of services delivered to devices as diverse as mobile phones, tablets, computers, appliances, and cars have become an increasingly important and integral part of our daily lives, in ways that could never have been envisioned as recently as five or ten years ago. These services provide the ability to communicate with friends, family, colleagues, external advisers and the world at large; to share and read live news from around the world or in-depth works of commentary and expression; and to engage in commerce whether shopping online, starting a business, or planning your next vacation or tonight's dinner. In sum, today the devices and the software that power them touch every aspect of our lives. For the companies operating in today's ever-connected digital world, the values of privacy, security, and transparency are essential guiding principles for building trust with their users. Indeed, the President focused on precisely these values in his Consumer Privacy Bill of Rights. *See* Executive Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 1 (2012) (noting that "[c]onsumers have a right" to "[t]ransparency" about "privacy and security practices" and the "secure and responsible handling of personal data").

The unprecedented scale of digital information used, stored and communicated on the Internet means that "privacy," which "has been at the heart of

our democracy from its inception," is "needed[] now more than ever." *Id* at C3. And courts repeatedly have recognized that as technology advances, individuals' expectations of privacy and transparency are *greater*, not lower. *See United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (en banc) ("Technology has the dual and conflicting capability to decrease privacy and augment the expectation of privacy."); *see also City of Ontario v. Quon*, 560 U.S. 746, 759 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."). As the Ninth Circuit, sitting en banc, recognized in *Cotterman*, the "uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy." 709 F.3d at 966.

Similarly, technological advances have created new cybersecurity risks, from hackers, identity thieves, and other criminal elements that threaten users' personal data, and the country's information security infrastructure and national interests. Companies' protection of users' data has become increasingly vital as more large-scale, sophisticated, and coordinated threats have emerged.

B. *Amici* Are Committed to Advancing These Core Values by Employing Security Technologies to Protect User Data, Acting Transparently, and Providing Users Control over Their Data

Amici are committed to advancing the core values of security, privacy, and transparency in the way they conduct their business and handle their users' data. They employ advanced security technology to protect users from external threats. The federal government and many states have pushed the private sector to take these steps, including through legislation and enforcement measures. As the FTC has observed, companies that maintain user data are potential targets for hackers and others, and therefore should incorporate security "into the decisionmaking in every department of [their] business." FED. TRADE COMM'N, START WITH SECURITY: LESSONS LEARNED FROM FTC CASES 2 (2015).

Further, *Amici* go to great lengths to disclose to their users how their data is

collected and protected so those users can make informed choices. They publish detailed privacy policies that inform users about security safeguards and the circumstances in which their data may be shared with others. *See, e.g.*, Twitter Privacy Policy, https://twitter.com/privacy; LinkedIn Privacy Policy, www.linkedin.com/legal/privacy-policy. *Amici* design their services to give users control over how their data is used, all to advance the important principles of privacy and transparency.

Finally, *Amici* inform their users that personal data may be disclosed in certain circumstances, including in response to lawful requests for user data, such as in law enforcement investigations. *See, e.g.*, eBay Privacy Policy, http://pages.ebay.com/help/policies/privacy-policy.html (noting that eBay cooperates with law enforcement and government agencies in response to verified requests relating to a criminal investigation or alleged or suspected illegal activity); LinkedIn Privacy Policy, *supra*, ¶ 2.6 (data may be disclosed to "comply with a legal requirement or process, including, but not limited to, civil and criminal subpoenas, court orders or other compulsory disclosures"); Twitter Privacy Policy, *supra* (similar). Several *Amici* also issue annual transparency reports, which disclose to users and the broader public the number and type of government requests for user data that have been made to them pursuant to lawful process.[1]

C. *Amici* Recognize and Respect the Government's Important Work Protecting Our National Security

In addition to committing to the values of privacy, security, and transparency, *Amici* routinely assist U.S. law enforcement in investigating crimes and threats to national security. They comply with proper, reasonable requests for data pursuant to

[1] *See, e.g.*, LinkedIn Transparency Report, https://www.linkedin.com/legal/transparency#government-requests; Twitter Transparency Report, https://transparency.twitter.com/country/us; Kickstarter Transparency Report, https://www.kickstarter.com/blog/kickstarter-transparency-report-2014; Twilio Transparency Report, https://www.twilio.com/legal/transparency.

valid legal process. As shown by the transparency reports of several *Amici*, they have provided information in response to numerous such requests.[2]

Amici's assistance with these investigations is conducted pursuant to clear rules, governed by applicable statutory and regulatory schemes and in accordance with the Constitution. These include the statutory requirements imposed on the government for obtaining a warrant or issuing a subpoena for user data in a company's possession. These established rules ensure transparency, predictability, and oversight. Absent such rules, there would be a serious risk that law enforcement could abuse its powers to obtain users' private information. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 859 (2004).[3]

D. The Government's Request Has No Legal Limits and Will Undermine Existing, Transparent Statutory Schemes that Reflect a Balancing of Competing Policy Considerations

As described in detail below (*see infra* at 14-25), the government's request in this case rests not on any specific statutory authorization, but on the novel theory that federal courts may use the All Writs Act to compel third parties to provide whatever assistance the government deems necessary or convenient in any particular investigation. In other words, the government seeks unbounded authority to compel Apple to design software that does not currently exist and that will circumvent and undermine security measures intended to protect its users' data. This principle could

---

[2] *See, e.g.,* Twitter Transparency Report for the United States, https://transparency.twitter.com/country/us (in second half of 2015 Twitter received 2,673 U.S. government requests for account information and produced information in response to 79%).

[3] When technology is rapidly changing, it is even more important that law enforcement operate pursuant to clear rules. That is because case-by-case judicial tests will quickly become obsolete as "the nature of the electronic devices that ordinary Americans carry on their persons continue to change." *Riley v. California*, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring); *see also* Kerr, *supra*, 102 Mich. L. Rev. at 858-59. As the Supreme Court has observed, "[t]he judiciary risks error by elaborating too fully" on the "implications of emerging technology before its role in society has become clear." *Quon*, 560 U.S. at 759.

require companies not just to turn over one user's information but to weaken security measures created to protect *all* users. Granting the government such extraordinary authority, without *any* set rules or legal protections, will not only erode user privacy and security and defeat users' interest in transparency, it will undermine an existing legislative framework balancing competing interests and policy considerations.

The government's demand, at its core, is unbound by any legal limits. It would set a dangerous precedent, creating a world in which the government could simply force companies to create, design, and redesign their systems to allow law enforcement access to data, instead of requiring the government to use the measures, and meet the requirements, of legislatively enacted statutory schemes. Nor is the fact that the government may claim that it does not plan to regularly exercise its far-reaching authority to commandeer software engineers of any comfort[4]: the creation or design of software in response to even one government order cannot be undone. *See Cotterman*, 709 F.3d at 966 (observing same about "unfettered dragnet effect" of warrantless border searches). Indeed, law enforcement officials already have indicated that if the government prevails in this case, they would seek to access *all* locked iPhones in their possession that are part of ongoing investigations.[5]

Likewise, the government's suggestion that steps could be taken to prevent

---

[4] Of course, it also must be emphasized that for several companies, particularly smaller ones, the burden in complying with such an order could be enormous. Apple itself has indicated that the burden on a company of its size would be substantial; for smaller companies that can only devote a handful of engineers to such a project the burden could be crippling to their ongoing operations.

[5] *See* Katie Benner & Matt Apuzzo, *Narrow Focus May Aid FBI in Apple Case*, N.Y. Times (Feb. 22, 2016), http://www.nytimes.com/2016/02/23/technology/apple-unlock-iphone-san-bernardino.html?_r=0 (New York City District Attorney Cyrus Vance responding "absolutely right" when asked whether he would seek to unlock nearly 175 iPhones in New York City law enforcement's possession); The Encryption Tightrope: Balancing Americans' Security and Privacy, YOUTUBE (March 1, 2016), https://www.youtube.com/watch?v=g1GgnbN9oNw&feature=youtu.be&t=3656 (FBI Director Comey responding "sure, potentially" when asked whether this case will "set a precedent" for law enforcement to seek the same assistance in other cases).

the disclosure of encryption-breaking software or limiting the circumstances in which it may force a company to build a backdoor, is of no reassurance. As the Second Circuit noted in the context of the NSA's self-imposed limits in its collection of bulk telephone metadata, the "more metadata the government collects and analyzes," the "greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals." *ACLU v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015). These kinds of concerns are particularly pronounced for companies like *Amici*, who securely store the personal data of, and handle massive volumes of Internet traffic for, over a billion users collectively.

Indeed, in assessing the constitutionality of warrantless GPS monitoring, Justice Sotomayor observed that granting the government "unfettered discretion" to obtain and use "a substantial quantum of intimate information" about citizens may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). Giving law enforcement the unprecedented power to force companies to design software to break their users' data protections, a power that is not bound by any legal or practical limit, presents precisely the same risk.

By contrast, in enacting existing statutory schemes governing law enforcement access to user data and digital communications—including Title III, the SCA, CALEA, and FISA—Congress weighed and balanced law enforcement needs with user security and privacy. *See infra* at 16-20.[6] By circumventing these processes and procedures, and the balance of policy considerations they reflect, the government seeks to avoid an essential public debate and do a judicial end-around the legislative framework that Congress carefully crafted.

Courts and scholars have emphasized that the public discourse afforded by

[6] This is not to say that *Amici* believe that the existing statutory scheme is perfect. But the fact that these laws are flawed in certain areas does not mean that the All Writs Act authorizes the broad sweeping powers suggested by the government here.

legislative rulemaking is essential for our society as we struggle with challenging questions about how far we should go in sacrificing liberty and privacy in protecting our national security. The Second Circuit affirmed the importance of robust debate of these questions last year when it held that the PATRIOT Act did not authorize bulk telephone metadata collection by the NSA. The court observed that while "expansive development of government repositories of formerly private records" and a corresponding "contraction of the privacy expectations of all Americans" could be "required by national security," "we would expect such a momentous decision to be preceded by substantial debate." *Clapper*, 785 F.3d at 818. Similarly, Justice Breyer has recognized the critical importance of public debate in resolving questions raised by the interplay between technology, national security, and privacy:

> Should cell phones be encrypted? Should web technology, making use of an individual's privacy preferences, automatically negotiate privacy rules with distant web sites as a condition of access? The complex nature of these problems calls for resolution through a form of participatory democracy. Ideally, that participatory process does not involve legislators, administrators, or judges imposing law from above. Rather, it involves law revision that bubbles up from below.

Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. Rev. 245, 263 (2002).

Likewise here, the government seeks an order that will "impose law from above" without considering the voices of the ordinary citizenry whose lives would be deeply affected by such relief.

E. Forcing Technology Companies to Break Their Own Security Measures Will Undermine User Confidence that Their Data Is Secure and Being Handled Transparently

If the government is able to compel companies to break their own security measures, the users of those companies will necessarily lose confidence that their data is being handled in a secure, open manner. The very security measures on which they have relied will have been compromised—and security "work arounds" created—by court order. Technological backdoors, whether or not built for specific and supposedly limited purposes, create an opportunity for criminals and hackers to

exploit. As security experts have observed, history has shown that no company can "build an access system that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document . . . . This is not theoretical; again and again, backdoor accesses built for one purpose have been surreptitiously used for another." Bruce Schneier, *Security or Surveillance?* (2016), https://www.schneier.com/essays/archives/2016/02/security_vs_surveill.html; Berkman Ctr. for Internet & Soc'y, *Don't Panic: Making Progress on the "Going Dark" Debate*, Appendix A to Landau (2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (noting, e.g., that "Vodafone built backdoor access into Greece's cell phone network for the Greek government; it was used against the Greek government in 2004-2005"). Moreover, forcing a company to undermine its own security measures provides a powerful disincentive to invest in security: firms could have no confidence that their carefully designed security systems would not be redesigned by court order.

In short, in addition to reducing the security of data and users' privacy, the government's demand here will force companies to violate existing representations to their users regarding access to, and the security of, their data, and will undermine their ability to make such assurances in the future. Similarly, the government could require companies to break other aspects of their agreements with users—by collecting more information than disclosed, sharing the data in undisclosed or unintended ways, or even surreptitiously forcing users to download code mandated by the government to weaken the privacy and safety protections promised to users. This would thwart users' legitimate expectations of privacy and security in their own information.[7] According to a recent Pew Report, 93% of Americans say that being in

[7] Indeed, the FTC has prosecuted companies it alleges used information in ways contrary to explicit promises in a privacy policy. *E.g.*, Press Release, Fed. Trade Comm'n, Gateway Learning Settles Privacy Charges (Jul. 7. 2004) ("You can change the rules but not after the game has been played.").

control of who can get information about them is important.[8] And if the government can force companies to break promises on issues as critical as data security and privacy, it may similarly "undo" other promises made to consumers to protect their privacy or other civil liberties, further eroding trust and confidence in their services.[9]

IV. THE GOVERNMENT LACKS THE AUTHORITY UNDER THE ALL WRITS ACT TO FORCE A PRIVATE PARTY TO RE-WRITE ITS SOFTWARE CODE AND SERVE AS AN INVESTIGATIVE ARM OF LAW ENFORCEMENT

As noted, Congress has enacted a number of statutes—including Title III, the SCA, CALEA, and FISA—that together comprehensively regulate the government's ability to acquire electronic communications and data, including from third-party companies. In enacting these laws, Congress balanced competing law-enforcement needs with user security and privacy, and ultimately chose *not* to give the government the very authority that it seeks here.

The All Writs Act is a procedural gap-filling measure designed to allow federal courts to effectuate powers they already have, not a broad independent grant of substantive power to federal courts. It cannot be used to circumvent the limitations established through the legislative process and the vital public debate accompanying it. And indeed, courts repeatedly have rejected similar efforts by the government to require third parties to provide forms of assistance not contemplated by statute. The Act does not grant the government the power Congress chose not to provide: the ability to require Apple to affirmatively rewrite its software code and undermine its own security systems to unlock a phone.

The cases cited by the government in its Motion to Compel do not support its

---

[8] Pew Research Center, Americans' Attitudes About Privacy, Security and Surveillance (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[9] In fact, this potential erosion of consumer trust puts undermines the entire Internet and technology industry, which has been a source of dynamic innovation and job creation in the U.S. economy. The critical foundation of that economic success has been the trust and confidence that consumers have placed in the sector.

case. They involve either an order (1) to turn over existing documents or data, or (2) to provide nonburdensome technical assistance to the government of a sort that already had been endorsed by Congress (e.g., pen registers and wiretaps) and that the third party already routinely performed outside the investigative context as part of its regular course of business. In none of these cases has a third party been compelled to take affirmative steps to create anything, much less sophisticated software designed to undermine its own security systems.

A. The All Writs Act Is a Gap-Filling Measure, Not a Broad Independent Grant of Substantive Power to Federal Courts

The All Writs Act permits federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651. The first Congress enacted the statute as part of the Judiciary Act of 1789, not to serve as a "'grant of plenary power to the federal courts,'" *Jackson v. Vasquez*, 1 F.3d 885, 889 (9th Cir. 1993), but rather as a "'legislatively approved source of procedural instruments'" designed to allow newly created federal courts to issue the writs necessary for them to perform the functions authorized by other laws. *Harris v. Nelson*, 394 U.S. 286, 299 (1969). In keeping with that original understanding, the Supreme Court's "view of the scope of the all writs provision" consistently has "confined it to filling the interstices of federal judicial power when those gaps threatened to thwart the otherwise proper exercise of federal courts jurisdiction." *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 41 (1985) (citing *McClung v. Silliman*, 19 U.S. (6 Wheat.) 598 (1821)).

The Supreme Court thus repeatedly has rebuffed efforts by litigants to use the All Writs Act in a manner that would circumvent or supplant other laws. "The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute. Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling." *Pa. Bureau of Corr.*, 474 U.S. at 43. The Act "does not authorize" federal courts "to issue ad hoc

writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *Id.* That is true *even where* the relevant statute does not expressly say that it provides the exclusive means by which a court may order the performance of the act at issue.

In *Pennsylvania Bureau of Corrections*, for instance, the Supreme Court held that the Act could not support a federal district court's order to the U.S. Marshals Service to transport potential witnesses in the custody of state corrections officials to federal court to testify in a pending § 1983 action. 474 U.S. at 43. Although no statute affirmatively said that the Marshals Service *did not* have such a duty, the Court reasoned that the federal habeas statutes, 28 U.S.C. §§ 2241, 2243, spoke to the issue of transportation of prisoners to court but provided "no basis . . . for a federal court to order the Marshals to transport state prisoners to the federal courthouse." 474 U.S. at 39. The Court concluded that the lack of specific statutory authority precluded the use of the All Writs Act to achieve that end.

Similarly, in *Carlisle v. United States*, 517 U.S. 416 (1996), the Supreme Court held that the All Writs Act could not support a district court's entry of a judgment of acquittal outside the time limit prescribed by Federal Rule of Criminal Procedure 29. *Id.* at 429. The Court had no difficulty concluding that Rule 29 "provide[d] the applicable law" and thus precluded the use of the All Writs Act to support entry of the judgment of acquittal, even though Rule 29 by its terms did not expressly say so. *Id.*[10]

B. Congress Has Enacted Several Statutes that Together Provide a Comprehensive Regulatory Regime Allowing the Government in Certain Circumstances to Obtain Assistance from Third Parties in the Course of Investigations, Displacing the All Writs Act

Here, Congress has left no procedural gaps for the All Writs Act to fill. Congress has enacted a number of statutes that create a comprehensive scheme

[10] *See also, e.g.*, *Syngenta Crop Protection, Inc. v. Henson*, 537 U.S. 28, 32-33 (2002) ("[p]etitioners may not, by resorting to the All Writs Act, avoid complying with the statutory requirements for removal"); *U.S. Alkali Export Ass'n v. United States*, 325 U.S. 196, 203 (1945) (writ of certiorari under All Writs Act could not serve as substitute for ordinary appeal authorized by statute).

regulating the government's ability to acquire electronic communications and data, including from third-party companies. In passing these statutes, Congress considered the relief the government requests in this action, but chose not to grant it. The All Writs Act may not be used to circumvent the requirements and limitations these statutes place on the government's ability to compel assistance in its investigations.

1. Congress's Decision to Prohibit Limits on Encryption and to Exclude Information Service Providers in CALEA Evidences Its Intent to Deny the Relief Sought by the Government

Of the statutes compelling third party assistance in law enforcement investigations—Title III, the SCA, FISA, and CALEA—only one (CALEA) mandates specific system-design requirements by third parties. These requirements generally obligate telecommunications carriers to design their systems in such a way as to facilitate the government's interception of real-time communications. *See* 47 U.S.C. § 1002(a)(1)-(4). Congress considered, and expressly declined to provide, the very authority the government seeks in this action.

First, even for telecommunications carriers covered by CALEA—which Apple and *Amici* are not—Congress denied law enforcement the right to dictate what security protocols, equipment, or operating standards should be employed. *See* 47 U.S.C. § 1002(b)(1). The House Report noted that this was "the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped." H.R. Rep. No. 103-827(I), at 19. This covered encryption:

> Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which *it does not retain the ability to decrypt communications for law enforcement access*. The bill does not address the "Clipper Chip"[11] or Key Escrow Encryption issue. Nothing in the

[11] The reference to the "Clipper Chip" was a 1994 proposal by the National Security Agency that involved installing a chip in cell phones that would allow the government to decrypt and intercept communications at will using a key escrow system. *See* Steven Levy, *Battle of the Clipper Chip*, N.Y. Times (June 12, 1994), http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

> bill is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, section 2602 protects the right to use encryption.

Id. at 24 (emphasis added). In other words, even within the highly regulated space of telecommunications carriers covered under CALEA, Congress protected the ability of companies to design their own technological systems. Under CALEA, a telephone company that encrypts its communications has *no* obligation to redesign its system so that law enforcement officers can make sense of intercepted transmissions.

Furthermore, as the text of CALEA makes plain (*see* 47 U.S.C. § 1002(b)(2)), in passing the statute Congress specifically chose *not* to impose any of these same system-design requirements on other entities, and in particular, information service providers *(id.* § 1001(6)), which encompass companies like Apple and several *Amici*. *See also* H.R. Rep. No. 103-827(I), at 18 (1994). That choice was deliberate. Congress considered and rejected proposed versions of CALEA that would have imposed such requirements:

> [P]rivate network systems or information services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems *do not have to be designed so as to comply with the capability requirements*. Only telecommunications carriers, as defined in the bill, are required to design and build their switching and transmission systems to comply with the legislated requirements. *Earlier digital telephony proposals covered all providers of electronic communications services, which meant every business and institution in the country. That broad approach was not practical. Nor was it justified to meet any law enforcement need.*

Id. (emphases added). This decision was motivated not only by practicality but also the significant privacy concerns at stake. The House Report observed that because "society's patterns of using electronic communications technology have changed dramatically" between the enactments of the SCA in 1986 and that of CALEA in 1994, stored electronic data "reveals a great deal about [individuals'] private lives,

all of it compiled in one place." *Id.* at 17. The fact that, eight years after imposing disclosure requirements on certain information service providers under the SCA, *all* information service providers were excluded from CALEA's scope is compelling evidence that Congress did not intend to allow the relief sought here. *See In re Apple, Inc.*, ___ F. Supp. 3d ___, 2016 WL 783565, at *10-11 (E.D.N.Y. Feb. 29, 2016). Indeed, in the years since CALEA was enacted, Congress has considered—and rejected—additional proposals to give the government the authority it now seeks to give itself via the All Writs Act. *See, e.g.*, Rep. Peter T. King, *Remembering the Lessons of 9/11*, 41 J. LEGIS. 173, 178 (2014-2015); *In re Apple, Inc.*, 2015 WL 5920207, at *3 (E.D.N.Y. Oct. 9, 2015).

The government does not contend that Apple has any obligation under CALEA to redesign its operating system. Indeed, it has not sought the remedies available under the statute, such as an order for non-compliance. Instead, it asks this Court to do exactly what Congress refused to do. But the Act cannot be invoked to grant the government powers Congress intentionally chose not to provide it.

2. Congress Has Placed Significant Limits on Law Enforcement's Ability to Compel Technical Assistance from Third Parties

Title III, the SCA, CALEA, and FISA all require certain providers of wire and electronic communications to offer technical assistance to law enforcement in certain circumstances. Such assistance includes interception of real-time communications, installation of pen registers and trap-and-trace devices, disclosure of stored communications, and investigations seeking "foreign intelligence information." *See* 18 U.S.C. §§ 2518(4), 2703(a)-(b), 3124(a)-(b); 47 U.S.C. § 1002(a)(4); 50 U.S.C. §§ 1802(a)(4)(A), 1822(a)(4)(a), 1842(d)(2)(B), 1861(c), 1881a(h)(1), 1881b(c)(5). Yet, as the government recognizes, none of these intricate statutes grants the powers the government seeks to arrogate to itself here.

Congress did *not* intend to give the government a blank check to compel law enforcement assistance from third parties—the precise consequence of the

government's interpretation of the All Writs Act. Indeed, in enacting the SCA, Congress recognized that consumers have a "reasonable expectation" that third party providers "will not become, in effect, a branch of Government law enforcement." S. Rep. No. 99-541, at 29 (1986). Any technical assistance requested pursuant to CALEA, Title III, or FISA must be provided with minimal interference to the services promised to customers. 18 U.S.C. § 2518(4); 47 U.S.C. § 1002(a)(4); 50 U.S.C. §§ 1802(a)(4)(A), 1805(c)(2)(B), 1822(a)(4)(A)(i), 1824(c)(2)(B), 1842(d)(2)(B)(i), 1881a(h)(1)(A), 1881b(c)(5)(B). For example, the Ninth Circuit has held that an eavesdropping request that, effectively, prohibited a vehicle monitoring system company from supplying "any of the various services it had promised its customer" violated 18 U.S.C. § 2518(4). *In re Application of U.S. for an Order Authorizing the Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1145-46 (9th Cir. 2003).

The government's effort to force Apple to redesign its operating system to facilitate surveillance runs afoul of these principles, which require a consideration not merely of the technical burden on the company, but also on users. The government's request would set a precedent that could be used in future cases to require *Amici* or others to provide technical assistance in a manner that undermines the very products they offer. At the very least, once Apple has written code to comply with the order, the government may seek orders to compel it to use such code over and over again. Congress has chosen not to give the government that authority, and the All Writs Act cannot be used to circumvent that limitation.

C. Courts Have Rejected Similar Efforts Under the All Writs Act to Compel Forms of Assistance that Are Not Contemplated by Statute

In keeping with the Act's role as a gap-filling measure rather than a broad substantive grant of power, courts repeatedly have rejected efforts by the government to require third parties to provide forms of novel technical assistance not contemplated by statute. Under this authority, the All Writs Act cannot support the government's request for an order to a company to rewrite its software code to

suit the government's preferences absent any statutory basis for that request.

The Ninth Circuit's decision in *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283 (9th Cir. 1979), illustrates the point. In *Plum Creek*, the Occupational Safety and Health Administration (OSHA) was trying to compel a lumber company's affirmative assistance in investigating whether environmental standards were being met by the company, and sought an order under the All Writs Act requiring the company to force its employees to wear certain environmental testing devices while on the job. *Id.* at 1285. Evidence showed that the devices were the most efficient method of measuring air quality and noise level, and while OSHA "could not guarantee that the testing devices would not cause any accidents," the risk of any harm resulting from their being worn was "minimal." *Id.* at 1286. The district court and Ninth Circuit nonetheless rejected OSHA's effort, and in particular concluded that the All Writs Act did not support the issuance of such an order. *Id.* at 1289-90.

The Ninth Circuit reasoned that the All Writs Act "permits the district court, in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers. It does not give the district court a roving commission to order a party subject to an investigation to accept additional risks at the bidding of OSHA inspectors." *Id.* at 1289. Even if the testing devices were the most efficient monitoring method, "in the absence of law specifying their use," the All Writs Act could not be used to "order Plum Creek to bear the added risks the devices would bring." *Id*. *Plum Creek* forecloses the government's request that this Court "usurp the legislative function," *id.* at 1290, and use a procedural gap-filling statute to require Apple to re-write its own software code and create potentially catastrophic risks to the security of users' Apple devices.

Plum Creek's holding finds support in more recent case law in which district courts have refused to allow the government to use the All Writs Act to require third parties to provide novel forms of assistance not contemplated by statute. In *In re Application of U.S.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005), the court held that the

All Writs Act could not support an order requiring a wireless provider to prospectively monitor and disclose to the government a suspect's location based on cell-tower data. The court concluded that this would be an "entirely unprecedented" use of the All Writs Act, and observed that Congress had spoken to the issue in Title III and the SCA, yet had not required companies to provide the type of assistance the government sought. *Id.* at 326. The court refused to "read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme." *Id.*

Likewise, in *In re Application of U.S.*, 849 F. Supp. 2d 526 (D. Md. 2011), the court rejected a similar effort by the government to use the All Writs Act to require a wireless provider to turn over real-time cell-tower location data pertaining to a particular suspect. The court concluded that existing statutory authority (namely the SCA) did not provide for this type of assistance, *id.* at 574-75, and that the Act could not be used to circumvent that detailed statutory scheme, *id.* at 582.

Indeed, in *In re Apple,* in a thorough analysis of the specific issue presented here, the district court declined to approve the government's request for an order commanding Apple to help unlock an iPhone. The court noted that Congress had opted not to give the government the specific authority it sought (2015 WL 5920207, at *1-3, 5), that it was "entirely possible, if not likely" that Apple had a "'substantial interest'" in not providing the assistance sought (*id.* at *5), and that the All Writs Act case law did not support the government's approach (*id.* at *7). The court reaffirmed and expanded upon these conclusions in a recent order, noting that the Act could not be used to compel Apple's assistance because the "legislative scheme" designed by Congress was "so comprehensive as to imply a prohibition against imposing requirements on private entities" that Congress had not "affirmatively prescribe[d]." *Apple*, 2016 WL 783565, at *9. This Court should adopt similar reasoning.

D. The Cases upon Which the Government Relies Do Not Support Forcing a Private Party to Create New Technology to Assist the Government's Investigation

The cases cited by the government in its Motion to Compel, as well as other cases in which courts have relied upon the All Writs Act to order private parties to assist government investigations, have not required a third party to take affirmative steps to create anything, much less to reengineer sophisticated software. These cases do not support what the government seeks to do here.

First, courts have used the All Writs Act to order third parties to turn over existing documents or data to the government to aid an investigation, in the same way as third parties routinely are required by subpoena to turn over documents or data discoverable in civil litigation. *See, e.g.*, *United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (ordering a credit card company to produce credit card records kept in the ordinary course of business); *In re Application of U.S. for an Order Directing X to Provide Access to Videotapes*, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (directing apartment complex operator "merely to provide access to surveillance tapes already in existence, rather than any substantive assistance, and nothing more"); *United States v. Doe*, 537 F. Supp. 838, 839-40 (E.D.N.Y. 1982) (directing telephone company to provide stored records of phone numbers dialed by suspect). These courts have emphasized the absence of any conceivable "adverse [e]ffect" on the third party associated with producing the records at issue. *Hall*, 583 F. Supp. at 719, 721 (noting that the "interest of the third party, Citibank, is not going to be affected by its compliance with this order, unless one argues that persons will not apply for Master Cards because those credit card records may be used by federal investigatory agencies"); *Videotapes*, 2003 WL 22053105, at *3 (noting that "[n]o costs will be incurred" in turning over videotapes, which "are readily available").

Second, courts have occasionally used the All Writs Act to order third parties to "provide nonburdensome technical assistance to law enforcement officers." *Plum Creek*, 608 F.2d at 1289. These cases—all of which involve telephone companies,

not hardware manufacturers, software developers, or other technology firms—do not support the government's attempt to invoke the All Writs Act in this case. In these cases, the assistance sought by the government was minor, amounting to no more than helping carry out a scaled-down version of a surveillance function already approved by Congress and that the company itself already performed in the regular course of its business. In none of the cases did the assistance sought entail any conceivable burden on the third party.

The government relies primarily on *United States v. New York Telephone Co.*, 434 U.S. 159 (1977). But that decision is a world removed from the circumstances in this case. There, the Supreme Court concluded that the Act could support an order to a telephone provider to assist with a pen register—i.e., to give the government a list of phone numbers dialed by a particular suspect. *Id.* at 174-78. But the Court went to great lengths to emphasize the limits of its holding. It noted that the "meager assistance" the government sought would not be "in any way burdensome" to the company, required only "minimal effort on the part of the Company," and entailed "no disruption to its operations." *Id.* at 174-75. Indeed, the company "concede[d] that it regularly employ[ed]" pen registers in the ordinary course of business "for the purposes of checking billing operations, detecting fraud, and preventing violations of law." *Id.* The Court also noted that the company was "a highly regulated public utility with a duty to serve the public," and could not claim to have a "substantial interest in not providing assistance." *Id.* at 174.

The *New York Telephone* Court also emphasized that the use of the All Writs Act to compel assistance with a pen register aligned with congressional intent. Through Title III, Congress "clearly intended to permit the use of pen registers by federal law enforcement officials." 434 U.S. at 176; *see also id.* at 165-68. Courts have recognized that as a "critical[] differen[ce]" between *New York Telephone* and cases, like this one, in which such congressional authorization is lacking. *In re Application of U.S.*, 849 F. Supp. 2d at 579.

Multiple other cases (several of which the government cites) are in the same vein: they approve the use of the All Writs Act to require the installation of pen registers or other similar surveillance devices already approved by Congress and routinely used by telephone companies in the ordinary course of business and for their own business purposes. *See, e.g.*, *In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129-30 (9th Cir. 1980) (approving use of All Writs Act to require phone company to assist with tracing numbers dialed from suspects' phones); *Application of U.S. for an Order Authorizing Installation of Pen Register*, 610 F.2d 1148, 1154 (3d Cir. 1979) (relying on *New York Telephone* in pen register case); *United States v. Mosko*, 654 F. Supp. 402 (D. Colo. 1987) (same); *In re Application of U.S. for an Order Directing a Provider of Commc'ns Servs. to Provide Tech. Assistance*, ___ F. Supp. 3d ___, 2015 WL 5233551 (D.P.R. Aug. 27, 2015) (phone company's assistance in consensual monitoring of electronic communication).

In only one (unreported) case has a court even *suggested* that the All Writs Act might appropriately be used as the government seeks here. *See In re XXX, Inc.*, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014). But, as explained by Apple (*see* Motion to Vacate [ECF No. 16] at 28), that opinion was issued without adversarial briefing, failed properly to analyze *New York Telephone*, misunderstood the type of technical assistance sought by the government, and by its own admission never considered the burden or adverse effect on the third-party company. Its reasoning, moreover, was comprehensively addressed and refuted by the district court in *In re Apple*, 2015 WL 5920207, at *4-7, which explains why *New York Telephone* and the other All Writs Act case law cannot support the government's approach here. *See also Apple*, 2016 WL 783565, at *17–27.

V. CONCLUSION

For the foregoing reasons, *Amici* respectfully urge the Court to deny the government's Motion to Compel and to grant Apple's Motion to Vacate.

DATED: March 3, 2016

Respectfully submitted,

MUNGER, TOLLES & OLSON LLP

By: 

JONATHAN H. BLAVIN

Attorneys for *Amici Curiae*