MICHAEL H. RUBIN, State Bar No. 214636
mrubin@wsgr.com
STEPHEN N. GIKOW, State Bar No. 302484
sgikow@wsgr.com
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1 Market Street
Spear Tower, Suite 3300
San Francisco, CA 94107
Telephone: (415) 947-2000
Facsimile: (415) 947-2099

BRIAN M. WILLEN, *Pro Hac Vice* Admission Forthcoming
bwillen@wsgr.com
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1301 Avenue of the Americas, 40th Floor
New York, NY 10019
Telephone: (212) 999-5800
Facsimile: (212) 999-5899

Attorneys for *Amicus Curiae*
Center for Democracy & Technology

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203.	ED No. CM 16-10 (SP) **BRIEF OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AS *AMICUS CURIAE* IN SUPPORT OF APPLE INC.'S MOTION TO VACATE AND IN OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE** **Hearing:** Date: March 22, 2016 Time: 1:00 p.m. Place: Courtroom 3 or 4 Judge: Hon. Sheri Pym

TABLE OF CONTENTS

Page

INTRODUCTION 1

INTEREST OF THE AMICUS 2

ARGUMENT 3

I. ORDERING A PRIVATE COMPANY TO DEFEAT ITS OWN SECURITY MEASURES BY CREATING A NEW VERSION OF ITS SOFTWARE IS AN IMPERMISSIBLE EXPANSION OF THE ALL WRITS ACT AND CONTRARY TO CONGRESS' DECISION TO WITHHOLD THAT POWER FROM LAW ENFORCEMENT 3

A. The Order the Government Seeks Is Not Allowed By the All Writs Act and Violates Apple's Constitutional Rights 4

B. The All Writs Act Cannot Be Used to Override Congress's Decision to Require Only Certain Kinds of Communications Providers to Include Backdoors in Their Technology 6

II. COMPELLING COMPANIES TO SUBVERT THEIR OWN SECURITY MEASURES WILL UNDERMINE PUBLIC TRUST IN CONNECTED DEVICES AND EMERGING TECHNOLOGIES 10

A. If the Government Wins This Case, a Wide Range of Other Technology Companies May Be Forced to Subvert Their Security Measures to the Detriment of Users Around the World 10

B. Giving the Government the New Power it Seeks Will Undermine User Trust and Legitimate Data Security in Concrete Ways 11

CONCLUSION 15

TABLE OF AUTHORITIES

Page(s)

CASES

Additive Controls & Measurement Sys. v. Flowdata, Inc., 96 F.3d 1390 (Fed. Cir. 1996) 4

In re Order Requiring Apple, Inc. To Assist In the Execution of a Search Warrant Issued By This Court, 15-MC-1902 (JO), 2015 U.S. Dist. LEXIS 138755 (E.D.N.Y. Oct. 9, 2015) 8-9

In re Order Requiring Apple, Inc. To Assist In the Execution of a Search Warrant Issued By This Court, 15-MC-1902 (JO) Dkt. 29, slip op. (E.D.N.Y. Feb. 29, 2016) ..... *passim*

In re United States ex rel. an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011) 4

In re United States for an Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 294 (E.D.N.Y 2005) ..... *passim*

ITT Cmty. Dev. Corp. v. Barton, 559 F.2d 1351 (5th Cir. 1978) 4

Pa. Bureau of Corr. v. United States Marshals Serv., 474 U.S. 34 (1985) 3, 6

U.S. Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000) 6

United States v. New York Tel. Co., 434 U.S. 159 (1977) 4

STATUTES

All Writs Act, 28 U.S.C. § 1651 ..... *passim*

Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001, *et. seq.* ..... *passim*

U.S. Const. amend. I 5

MISCELLANEOUS

"ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk" (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put 12

Barbara Guttman and Edward Roback, *An Introduction to Computer Security: The NIST Handbook*, National Insitute of Standards and Technology, Special Publication 800-12 (October 1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (last visited March 2, 2016) 5

CALEA II: Risks of Wiretap Modifications to Endpoints (May 17, 2013), *available at* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf 8, 9

Comments of the Center for Democracy & Technology on the Use of Encryption and Anonymity in Digital Communications, as submitted to the United Nations (Feb. 13, 2015), *available at* https://cdt.org/files/2015/02/CDT-comments-on-the-use-of-encryption-and-anonymity-in-digital-communcations.pdf 11

Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and and espionage costs $445 billion annually," *Wash. Post* (June 9, 2014), https://.washingtonpost.com/world/security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html 14

Ellen Nakashima, "Former national security officials urge government to embrace rise of encryption," *Wash. Post*. (Dec. 15, 2015), https://www.washingtonpost.com/world/national-security/former-national-security-officials-urge-government-to-embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-9c4e-be37f66848bb_story.html?hpid=hp_regional-hp-cards_no-name%3Ahomepage%2Fcard 14-15

Going Dark: Encryption, Technology, and the balance Between Public Safety and Privacy, S. Comm. on the Judiciary, 114th Cong. (Jul. 8, 2015) 7, 8

Government Accountability Office, *Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, http://www.gao.gov/new.items/d031138t.pdf 13

Harold Abelson et. al., Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications 17 (July 6, 2015), *available at* https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf 15

"Issue Brief: A "Backdoor" to Encryption for Government Surveillance," *Center for Democracy & Technology* (Dec. 15, 2015), https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/ 8

Nicole Perlroth and David E. Singer, "Obama Won't Seek Access to Encrypted User Data," *New York Times* (Oct. 10, 2015), http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html 8, 15

Press Release (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices 12

"Read the Obama administration's draft paper on technical options for the encryption debate," *Wash. Post* (last visited Mar. 2, 2016), http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/.....13

INTRODUCTION

As a nation, we are stunned and saddened when there are inexplicable attacks on innocent victims, and the tragedy in San Bernardino is no exception.

But the issues in this case go far beyond this one investigation or a single phone. This case is about giving the government the power to conscript technology providers to create new versions of their products intended solely to defeat the security features designed to safeguard their users. It is about minimizing technological vulnerabilities that could be exploited to the detriment of everyone who uses connected devices. A decision in favor of the government would set the stage for similar orders against a wide range of technology companies and all manner of products. It would set a precedent under which any company could be forced to spy on unknowing customers on behalf of law enforcement, and in the process be required to override its own security measures in ways that expose its users to malicious attacks. All of this could be done behind closed doors, *ex parte*, with little or no opportunity for the company or public to be heard.

We live in a world that is increasingly interconnected. You can monitor your sleeping baby through a webcam. You can use your phone to adjust your thermostat on your drive home and then use it to turn on your house lights. You can receive messages on your phone if your carbon monoxide alarm goes off. Your medical devices can make an emergency call for help if you become incapacitated. These are amazing and positive developments for the human experience, and they better our lives.

But these systems need to be safe from malicious third party attacks. A decision compelling Apple to weaken critical security features on its phones will leave the creators of a wide range of Internet-connected consumer products—cars, televisions, personal fitness trackers, even refrigerators and home security systems—vulnerable not only to government conscription by the United States and foreign regimes, but also to malicious attacks by criminals, state actors, and even terrorists.

When your whole house is capable of listening to you, poor security features on these connected devices mean that you will have no control over who is hearing your most private moments. And this will have been enabled by the very companies that create this technology, work hard to make it secure, and in whom users must necessarily put their trust. If the government succeeds in this case, the relationship between technology providers and users will be forever altered. Users will never know whether the companies whose products they use have been conscripted by the government to break the essential privacy and security features that are supposed to protect them.

That is not a world that this Court should welcome. And it is certainly not one that should be created by judges acting without clear statutory authorization. The Court should grant Apple's motion to quash and deny the government's motion to compel.

INTEREST OF THE AMICUS

The Center for Democracy & Technology ("CDT") is a nonprofit advocacy organization that works to ensure that the human rights we enjoy in the physical world are realized online and that technology continues to serve as an empowering force for people worldwide. Integral to this work is CDT's representation of the public interest in the creation of an open, innovative, and decentralized Internet that promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

CDT was formed in 1994 as part of civil society's efforts to push back against the backdoors mandated by the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001, *et. seq.* ("CALEA"), a statute directly relevant to this case and discussed in greater detail below. More than 20 years later, the public conversation on these important issues continues, as technology rapidly expands into every portion of our lives. CDT advocates for strong online security and privacy protections, which are essential to building the trust necessary for individ-

uals to adopt new technologies and access the multitude of benefits of an increasingly interconnected world while also maintaining privacy in their most personal communications, associations, interests, and activities. CDT is keenly aware of the consequences of allowing the government to force private companies to break the very security features they designed, and for that reason it has been a key participant in resisting efforts to expand CALEA to require technology providers like Apple to create backdoors in their products for the benefit of law enforcement.

This case squarely implicates these concerns. CDT submits this *amicus curiae* brief to urge the Court to confine the All Writs Act to the limited purpose for which it was intended and to make clear the government does not have the power to use the courts to conscript technology companies into the unauthorized service of law enforcement.

ARGUMENT

I. ORDERING A PRIVATE COMPANY TO DEFEAT ITS OWN SECURITY MEASURES BY CREATING A NEW VERSION OF ITS SOFTWARE IS AN IMPERMISSIBLE EXPANSION OF THE ALL WRITS ACT AND CONTRARY TO CONGRESS' DECISION TO WITHHOLD THAT POWER FROM LAW ENFORCEMENT

The All Writs Act was enacted in 1789 for the limited purpose of allowing the federal courts to issue auxiliary writs as needed to protect their jurisdiction. *Pa. Bureau of Corr. v. United States Marshals Serv.*, 474 U.S. 34, 41-43 (1985). The government now asks the Court to apply this old and narrow statute in a bold and novel way: to order a private company to write new software designed to allow the government to break the security features that the company has designed for the protection of its users. This would transform a statute designed to help fill the interstices of federal judicial power into an expansive tool for law enforcement officers to obtain substantive new powers—powers that Congress has, for good reason, declined to convey.

A. The Order the Government Seeks Is Not Allowed By the All Writs Act and Violates Apple's Constitutional Rights

The order the government seeks in this case appears to be unprecedented. No court has ever used the All Writs Act to conscript a private company to create a brand new version of one of its products solely to defeat its own security measures. To apply the Act in this novel way would stretch what is supposed to be a narrow, gap-filling statute, with only limited application to third parties, beyond all measure. "Nothing ... suggests that the All Writs Act can be employed as a general license for district courts to grant relief against non-parties whenever such measures seem useful or efficient." *Additive Controls & Measurement Sys. v. Flowdata, Inc.*, 96 F.3d 1390, 1396 (Fed. Cir. 1996); *see also In re United States ex rel. an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 580 (D. Md. 2011) ("The fact that a party may be assisted in its discharge of its rights or duties by the issuance of a writ is not a sufficient basis for the writ.") (citing *ITT Cmty. Dev. Corp. v. Barton*, 559 F.2d 1351, 1360 (5th Cir. 1978). Indeed, what the government would inflict on Apple are precisely the "unreasonable burdens" that "may not be imposed" on third parties. *United States v. New York Tel. Co.*, 434 U.S. 159, 172 (1977).

A fitting response to the government's request was supplied a decade ago in another case where the All Writs Act was improperly invoked to justify the use of a broad new investigative tool:

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

> judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority.

In re United States for an Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 294, 326 (E.D.N.Y 2005) ("*In re Pen Register*"). This understanding of the proper judicial role in applying the All Writs Act was echoed earlier this week, when a federal court in New York rejected the government's application for an order requiring Apple to bypass the security on one of its devices. *In re Order Requiring Apple, Inc. To Assist In the Execution of a Search Warrant Issued By This Court*, 15-MC-1902 (JO) Dkt. 29 (E.D.N.Y. Feb. 29, 2016) ("*In re Apple Order*"). As Judge Orenstein explained, "what the government seeks here is to have the court give it authority that Congress chose not to confer." *Id*., slip op. at 30. That is even more true in this case.

Indeed, what the government seeks in this case would violate Apple's constitutional rights under the First Amendment. The order at issue would not merely force Apple into an act of creative code writing, it would require the company to speak in ways contrary to its basic principles and values, and in a manner that undermines previous assurances the company has given its customers about the security controls of its product. To comply, the company would have to "create a brand new product that impairs the utility of the products it is in the business of selling." *In re Apple Order*, slip op. at 28. On top of that, Apple would have to authenticate the newly created software using its own cryptographic "signature," thereby verifying as trustworthy a piece of code that the company considers to be malware.[1] This

[1] "An electronic signature is a cryptographic mechanism that performs a similar function as a written signature. It is used to verify the origin and contents of a message. For example, a recipient of data (e.g., an email message) can verify who signed the data and that the data was not modified after being signed. This also means that the originator (e.g., sender of an email message) cannot falsely deny having signed the data." Barbara Guttman and Edward Roback, *An Introduction to Computer Security: The NIST Handbook*, National Insitute of Standards and Technology, Special Publication 800-12 (October 1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (last visited March 2, 2016).

kind of compelled speech is inconsistent with the First Amendment. A basic requirement for any order issued under the All Writs Act is that it must be "agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). The order at issue here is nothing of the sort.[2]

B. The All Writs Act Cannot Be Used to Override Congress's Decision to Require Only Certain Kinds of Communications Providers to Include Backdoors in Their Technology

"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. That is the situation here. Over the past several decades, Congress, the Executive Branch, law enforcement, the private sector, and CDT and other public-interest groups have been engaged in dialogue over precisely the issues raised by this case: whether, and under what circumstances, providers of communications technology, device manufacturers, and software developers should be required to create "backdoors" that facilitate the government's ability to search those products.

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"). The Act "requires telecommunications carriers and equipment manufacturers to build into their networks technical capabilities to assist law enforcement with authorized interception of communications and 'call-identifying information.'" *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000) (quoting 47 U.S.C. § 1002). The process that produced CALEA allowed various stakeholders—including CDT—to participate, and the law itself was the product of negotiation between those various interests. The resulting statute requires "telecommunications carriers" to design their systems in ways that preserve

[2] Apple and other amici are ably briefing the multitude of constitutional concerns raised by this case. CDT shares in these concerns.

the government's ability to intercept certain communications (47 U.S.C. § 1002(a)) but deliberately withholds obligations to facilitate government surveillance efforts from other kinds of providers.

Among the providers that are expressly excluded from CALEA's mandates are "information services" such as Apple (*id.* § 1002(b)(2)). *See In re Apple Order*, slip op. at 16-17. Not only that, CALEA "provides that law enforcement agencies cannot do precisely what the government suggests here: dictate to a private company in the business of manufacturing smartphones the extent to which it may install data security features on such devices." *Id.* at 35 n.29 (citing 47 U.S.C. § 1002(b)(1)(b)).

While CALEA is imperfect, it reflects a clear legislative choice about what kinds of service providers should—and should not—be compelled to provide private assistance for law enforcement. Indeed, as Judge Orenstein has explained, the "absence from that comprehensive scheme of any requirement that Apple provide the assistance sought here implies a legislative decision to prohibit the imposition of such a duty." *In re Apple Order*, slip op. at 20. Congress's decision leaves no room for the All Writs Act.

The impropriety of using that general statute to recalibrate the balance struck by Congress is underscored by more recent events. In the last few years there has been considerable public debate about whether to expand CALEA to impose obligations on providers like Apple that were excluded from the statute's original mandates. In 2015, Congress held hearings addressing whether new legislation should be enacted to require device manufacturers (including Apple) and other providers of emerging technologies to include backdoors in their products to cover cases much like this one. *Going Dark: Encryption, Technology, and the balance Between Public Safety and Privacy*, S. Comm. on the Judiciary, 114th Cong. (Jul. 8, 2015). This process allowed the relevant stakeholders to make their case. *See,*

e.g., *id.* (statements of Deputy Attorney General Sally Quillian Yates and FBI Director James B. Comey).

CDT, and many other interested parties, spoke out against those proposals, arguing that incorporating backdoors would fundamentally weaken security features that are designed to protect users from hackers and other unlawful intruders, both domestic and foreign. *See* "Issue Brief: A "Backdoor" to Encryption for Government Surveillance," *Center for Democracy & Technology* (Dec. 15, 2015), https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/. In a report coordinated by CDT, for example, a group of leading cryptographers and security researchers explained that:

> [The] FBI's desire to expand CALEA mandates amounts to developing for our adversaries capabilities that they may not have the competence, access, or resources to develop on their own. In that sense, the endpoint wiretap mandate of CALEA II may lower the already low barriers to successful cybersecurity attacks.

CALEA II: Risks of Wiretap Modifications to Endpoints at 7 (May 17, 2013), *available at* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

After considering these arguments, the Obama Administration ultimately decided not to seek legislation. *See* Nicole Perlroth and David E. Singer, "Obama Won't Seek Access to Encrypted User Data," *New York Times*, (Oct. 10, 2015), http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html. In making that decision, the Administration concluded "that an effort to compel the companies to give the government access would fail, both politically and technologically." *Id.*; *see also In re Order Requiring Apple, Inc. To Assist In the Execution of a Search Warrant Issued By This Court*, 15-MC-1902 (JO), 2015 U.S. Dist. LEXIS 138755, at *9-10 (E.D.N.Y. Oct. 9, 2015) (explaining that "members of the executive and legislative branches have considered updating [CALEA] to allow, among other things, the judicial authorization of the

precise investigative technique at issue here—and have not reached a consensus that such action is warranted").

In this case, however, the government acts as if this debate, and the resulting decisions by the political branches, never happened. Instead, the FBI asks the Court to use the All Writs Act to give it a power that was deliberately withheld in the legislative arena. In fact, the authority that the government now seeks here is broader than anything contemplated in the theoretical CALEA II, because it would force companies to create new versions of products that are already in the market—versions specifically designed to undo security features built into those products and relied upon by the consumers who purchased them.

This is an entirely unwarranted expansion of the All Writs Act. The Act is not "a mechanism for the judiciary to give [the government] the investigative tools that Congress has not." *In re Pen Register*, 396 F. Supp. 2d at 325. There is good reason for that rule. Sensitive and important public policy questions are properly left to specific statutes that can balance competing concerns, rather than be resolved in an ad hoc manner citing a general statute enacted centuries ago for an entirely different purpose. Indeed, it is at odds with basic separation-of-powers principles to allow the Executive to circumvent the give-and-take of the legislative process by seeking authority from the courts, often in proceedings "shielded from public scrutiny." *In re Apple Order*, slip op. at 29.

That is especially so here, where the relevant legislative debate has already occurred and Congress has decided not to give law enforcement the kind of power it seeks here without any meaningful statutory authorization. In such cases, the courts rightly decline any invitation to "transform the AWA from a limited gap-filling statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by Congress's superior ability to prohibit or

preempt." *Id.* at 26. To do otherwise would be "an exercise of judicial activism that is breathtaking in its scope." *In re Pen Register*, 396 F. Supp. 2d at 326.

II. COMPELLING COMPANIES TO SUBVERT THEIR OWN SECURITY MEASURES WILL UNDERMINE PUBLIC TRUST IN CONNECTED DEVICES AND EMERGING TECHNOLOGIES

The government pretends that this case is only about a single investigation and a solitary iPhone used by a deceased killer. But the expansive power that the government is seeking cannot be limited to a single company, and certainly not to one person's phone. Compelling Apple to write software to defeat its own security and to facilitate the hacking of its technology will set the stage for similar requests aimed at a wide range of other providers and other devices. That will have far-reaching consequences. Allowing the government to force technology companies to rewrite or rewire their products at the direction of law enforcement will fundamentally alter the relationship between those companies and their users. It will erode public trust across a variety of devices and applications. This will make those technologies—and those who use them—less secure, not just from the government but from hackers, thieves, and repressive regimes.

A. If the Government Wins This Case, a Wide Range of Other Technology Companies May Be Forced to Subvert Their Security Measures to the Detriment of Users Around the World

Although this case may concern a single company and a single smartphone, the potential impact of this Court's decision is far broader. People now use a wide variety of advanced, Internet-enabled technologies. Once a precedent is established that the All Writs Act can be used to force companies to break their own products, any of these devices could be subject to a similar order. This has startling implications for security and privacy across a wide range of emerging technologies.

The government might next try to obtain an order requiring a smart TV manufacturer to write new code that uses the television's voice-recognition technology to record and report back what is being said in a customer's living room. Or the government could conscript a home-security company to issue a software up-

date to an in-home camera that would suddenly allow government agents to watch the homeowner's every move. A court order could likewise require a wearable fitness company to hijack a GPS-enabled fitness tracker, reporting to the government real-time data about the wearer's location. These companies would be compelled by law enforcement to defeat the very aspects of their products that are supposed to protect users' privacy and security.

The result of all this would be profound. Citizens would be increasingly vulnerable to cybercriminals and others seeking to put their weakened devices to illicit use. Some of the most vulnerable users of connected technologies, who heavily rely on those technologies' privacy and security features, are those doing work in the public interest: human rights activists, advocates, journalists, and others. These individuals place a premium on secure communications and data because they face such obvious dangers from repressive regimes and others intent on thwarting their activities. Weakening the technology that they rely on to do their jobs may expose them to great harm, as well as deter others from taking on this important work. *See* Comments of the Center for Democracy & Technology on the Use of Encryption and Anonymity in Digital Communications, as submitted to the United Nations (Feb. 13, 2015), *available at* https://cdt.org/files/2015/02/CDT-comments-on-the-use-of-encryption-and-anonymity-in-digital-communcations.pdf.

B. Giving the Government the New Power it Seeks Will Undermine User Trust and Legitimate Data Security in Concrete Ways

In an increasingly connected world, security is the predicate to all of our digital lives. Businesses rely on the security of information to keep their customers' data safe and their own information out of the hands of competitors and criminals. Similar protections allow doctors to meet virtually with patients around the world; they give online shoppers the confidence to send payment information to their favorite stores; they allow curious college students to be comfortable enough to search for and read unpopular opinions; they are necessary features of any baby

monitor. As the Chairwoman of the FTC noted: "The only way for the Internet of Things to reach its full potential for innovation is with the trust of American consumers." Press Release (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

Unsurprisingly, therefore, technology companies devote considerable resources to developing and implementing security and privacy features on their products. They make representations about those features to consumers and regulators, which help set consumer expectations about how technology works and what protections they provide to users.[3] Now, however, the FBI seeks to destabilize this dynamic by demanding the power to force these same companies to create new versions of their products that would undermine the very features that are supposed to protect users and safeguard their information. That would profoundly undermine companies' relationships with their users.

How can people trust that the security features protecting the technologies they rely on for work, education, friendship, and romance will actually keep them secure if the government can force the same company who designs the product to break it? This is a profound disruption. The public generally has to take on faith that a given product or software update is secure: users are often not in a position to independently verify the security of their devices or every software update. That faith comes from a company's statements about its products and from that company's history and reputation. By making companies into adjuncts of law enforcement and compelling them to create new versions of their own products that defeat

[3] Indeed, government agencies, including the Federal Trade Commission and the Federal Communications Commission, stand ready to hold the private sector accountable for the promises they make about the security of their devices and, in some cases, to require them to adopt certain kinds of security or data-protection features. *See, e.g.,* "ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk" (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

existing security and privacy features—but that still come with the company's cryptographic seal of approval—the order the government seeks here will directly undermine that trust. When companies are forced to deceive their customers and push out software updates for the benefit of law enforcement rather than for the good of their users, those users will naturally come to distrust what those companies say and look skeptically at any new version of their products.

Disrupting the trust between technology providers and their users will have real consequences, which are likely to be felt in several different ways.

First, users may be less willing to update the software on their devices, which in turn will make those devices less secure over time. Software updates are essential for keeping technology up-to-date, with the latest patches fixing the most recent security vulnerabilities. Government Accountability Office, *Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, http://www.gao.gov/new.items/d031138t.pdf. There is serious concern that granting orders like the one at issue here will diminish trust in such updates more generally. Indeed, the Obama Administration's own working group worried about this very thing. It explained that enabling "remote access to encrypted devices through current update procedures ... could call into question the trustworthiness of established software update channels," which in turn might lead individuals "to turn off software updates, rendering their devices significantly less secure as time passed and vulnerabilities were discovered by [sic] not patched." "Read the Obama administration's draft paper on technical options for the encryption debate," *Wash. Post* at 6 (last visited Mar. 2, 2016), http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/. The order that the government seeks against Apple highlights this very problem. As explained above, the order requires Apple to issue a new software update designed specifically to undermine the company's existing security features. In order for the target device to accept the update, Apple would need to

verify the government-mandated update using its cryptographic signature. That signature acts as a "wax seal" on the envelope containing the software update: it tells users that the software update came from Apple and is safe to install. But if the government can force Apple to sign software as legitimate that Apple actually considers to be untrustworthy malware, it would call into question all future software updates and cryptographic signatures, not just from Apple but from other technology companies that may be subject to similar orders. If users distrustful of government-mandated updates decline to install software updates more generally, it would leave a cluster of these "unpatched" devices, which would be prime targets for criminals, malicious hackers, and others with nefarious intent. The existence of those devices would make other connected devices and even whole networks more vulnerable. Reports estimate that the U.S. already loses $100 billion to cybercrime every year. Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and espionage costs $445 billion annually," *Wash. Post* (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html. By fostering this dangerous dynamic, the order the government seeks would help create a landscape even more ripe for such abuse.

Second, if the U.S. government can demand these kinds of backdoors, other governments more repressive and less restrained than our own will surely demand them as well. This danger will make our technological infrastructure weaker and more susceptible to foreign espionage and cyberattack.[4] That is one important reason why a respected group of former intelligence officers have argued that the FBI is wrong to seek backdoor access to U.S. companies' technology. Ellen

[4] Fear of other governments gaining similar access was one of the main reasons that the Obama Administration decided not to seek legislation requiring the very kind of backdoor that the FBI is seeking here to exploit. *See* Perlroth and Singer, *supra*.

Nakashima, "Former national security officials urge government to embrace rise of encryption," *Wash. Post.* (Dec. 15, 2015), https://www.washingtonpost.com/world/national-security/former-national-security-officials-urge-government-to-embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-9c4e-be37f66848bb_story.html.

Third, if they are unable to trust that American technology providers are not working behind the scenes to undermine their own products at the government's behest, people may turn to foreign products that are seen as more secure and less vulnerable to hacking mandated by American law enforcement officers. Former CIA director and NSA head Michael V. Hayden has expressed concern about this exact problem, which he calls "the worst of all worlds: there will be unbreakable encryption—it just won't be made by American firms." Nakashima, "Former national security officials urge government to embrace rise of encryption," *supra*. Not only would this undermine the interests of U.S. law enforcement, it would be a major blow to the U.S. companies that produce these technologies—companies that are currently worldwide leaders but might see their positions slip as consumers seek hardware and software elsewhere. *See, e.g.*, Harold Abelson et. al., Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications 17 (July 6, 2015), *available at* https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

CONCLUSION

The Court has been asked to give law enforcement officials a broad new power to compel private businesses to speak by writing—and ratifying as trustworthy—software designed to circumvent their own security measures. The members of the First Congress who drafted the All Writs Act—patriots for whom the experience of overbearing royal authority was still fresh in the mind—could hardly have imagined such an application of the statute. This case threatens to dramatically un-

dermine all of our safety and privacy. The government's motion to compel should be denied, and Apple's motion to vacate granted.

Dated: March 3, 2016

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: _____
Michael H. Rubin

Attorneys for *Amicus Curiae*
Center for Democracy & Technology