Mark E. Haddad, SBN 205945
mhaddad@sidley.com
SIDLEY AUSTIN LLP
555 West Fifth Street, Suite 4000
Los Angeles, California 90013
Telephone: +1 213 896-6000
Facsimile: +1 213 896-6600

Eamon P. Joyce (*pro hac vice* motion forthcoming)
ejoyce@sidley.com
Nicholas M. McLean (*pro hac vice* motion forthcoming)
SIDLEY AUSTIN LLP
787 Seventh Avenue
New York, New York 10019
Telephone: +1 212 839-5300
Facsimile: +1 212 839-5599

Attorneys for *Amicus Curiae* ACT | The App Association

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

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

Case No. 5:16-CM-00010 SP

BRIEF OF *AMICUS CURIAE* ACT |
THE APP ASSOCIATION IN
SUPPORT OF APPLE INC.'S
MOTION TO VACATE ORDER
COMPELLING ASSISTANCE

Date: March 22, 2016
Time: 1:00 p.m.
Place: Courtroom 3 or 4
Judge: The Hon. Sheri Pym

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Julia Angwin, *What's Really at Stake in the Apple Encryption Debate*, ProPublica (Feb. 24, 2016), https://www.propublica.org/article/whats-really-at-stake-in-the-apple-encryption-debate 20

Apple, *Unauthorized Modification of iOS Can Cause Security Vulnerabilities, Instability, Shortened Battery Life, and Other Issues* (Sept. 22, 2015), https://support.apple.com/en-us/HT201954 16

Catherine Barrett, *Healthcare Providers May Violate HIPAA by Using Mobile Devices to Communicate with Patients*, 8 ABA Health *e*Source, no. 2 (Oct. 2011), http://www.americanbar.org/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1110_barrett.html 3

Brad Chacos, *Here's How to Best Secure Your Data Now That the NSA Can Crack Almost Any Encryption*, PC World (Sept. 6, 2013), http://www.pcworld.com/article/2048248/heres-how-to-best-secure-your-data-now-that-the-nsa-can-crack-almost-any-encryption.html 6

Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547 (1999) 16

The Encryption Tightrope: Balancing Americans' Security and Privacy, H. Comm. on the Judiciary, 114th Cong. (2016), http://judiciary.house.gov/index.cfm/2016/3/the-encryption-tightrope-balancing-americans-security-and-privacy 24

Ernst & Young, *Bring Your Own Device: Security and Risk Considerations for Your Mobile Device Program*, Insights on Governance, Risk & Compliance (Sept. 2013), http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf 4

Federal Communications Commission, *Cyber Security Planning Guide*, https://transition.fcc.gov/cyber/cyberplanner.pdf 2, 4

Federal Trade Commission, *What's the Deal? An FTC Study on Mobile Shopping Apps* (2014), https://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf 7, 19

Jim Finkle, *Solid Support for Apple in iPhone Encryption Fight: Poll*, Reuters (Feb. 24, 2016), http://www.reuters.com/article/us-apple-encryption-poll-idUSKCN0VX159........24

Tomio Geron, *Something Ventured: Uncle Sam Is Staking Start-Ups*, VentureWire (Mar. 12, 2008)........7

Heidi Hoopes, *Apps to Easily Encrypt Your Text Messaging and Mobile Calls*, Gizmag (Sept. 27, 2014), http://www.gizmag.com/secure-text-messaging-phone-clients-comparison-ios-and-android/34000........6

Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403 (2013)........3

Rather than restating the arguments Apple Inc. ("Apple") has made in its Motion to Vacate the Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to the Government's Motion to Compel Assistance (filed Feb. 25, 2016) [ECF Docket Entry 16] (hereinafter "Apple's Mot."), *amicus curiae* ACT | The App Association ("ACT") writes narrowly to emphasize the enormous burdens that the Government's position would impose on software developers, and to discuss the potential damage such a position threatens to inflict on a significant and growing sector of the U.S. economy.

BACKGROUND

Just one tool to protect privacy and security is directly implicated in this case, but what the Government seeks to do would send rippling effects through the entire digital economy, particularly for those who develop software for the mobile economy. This case involves the Government's ability to dictate to any company that it has to write code for any purpose that potentially would facilitate a law enforcement investigation. That, as we explain below, would impose an untenable burden on the App Economy, which now is a vital sector of the nation's overall economy and continues to unleash an extraordinary wave of innovation and expansion. In 2012, "[t]he App Economy [was] responsible for roughly 466,000 jobs in the United States, up from zero in 2007." Michael Mandel, *Where the Jobs Are: The App Economy* 1 (2012).[1] Today, that number is closer to 1.7 million. *See* Michael Mandel, *App Economy Jobs in the United States (Part 1)*, Progressive Pol'y Inst. (Jan. 6, 2016). This $120 billion industry is led by U.S. companies, the vast majority of which are startups or small businesses. *See* ACT, *State of the App Economy* 4 (4th ed. 2016).

As the App Economy has grown, so have the demands and expectations of consumers and businesses for privacy and security in connection with their transac-

[1] For ease of reading, *amicus curiae* omits URL citations from the body of this brief. The URLs at which to access the cited authorities appear in the Table of Authorities.

tions and communications. In a dynamic economy in which consumer trust is essential (and easily lost), businesses are increasingly bundling encryption and other forms of data protection with their products. Privacy and security, therefore, are industry best practices and essential competitive advantages. Any electronic platform that allows two-way communication must think about privacy and security, and any platform that seeks to allow anonymity (for any purpose) must do the same. Thus, against this backdrop, companies have adopted a variety of digital security initiatives to protect data. Encryption, at the fore here, has become an integral part of the U.S. economy: It provides the transaction security that allows companies to sell globally and provides security for much of the nation's commerce, and ensures that our most sensitive data stays private—protecting patient health information, financial data, and every American who shops online. *See*, *e.g.*, Federal Communications Commission ("FCC"), *Cyber Security Planning Guide*, at PDS-4 ("The two primary safeguards for data are passwords and encryption."). But there are many other means for securing digital information in addition to encryption and the specific processes implicated by the Government's request for assistance here. Software companies design programs that, *inter alia*, limit access to data stored or collected by software, or that purge data automatically after a set period (perhaps most famous is Snapchat, whereby photos and messages are automatically deleted shortly after receipt).

Such privacy and security protections are vital to the mobile economy. As the United States Supreme Court has recognized, "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). "Today, . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Id.* at 2490. "Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life."

Id. Platform designers, telecom providers, and third-party software developers, working together, have created the App Economy in less than a decade, and "[t]he mantra of the smart phone era is that 'there's an app for that,' indicating that there is a program to fulfill every need." Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403, 405 (2013).

With mobile platforms and communications now ubiquitous, risks that private data will be breached have multiplied. To start, "[m]obile devices are particularly vulnerable to loss and theft because of their small size and portability. The most common form of security breach is the theft of mobile devices." Catherine Barrett, *Healthcare Providers May Violate HIPAA by Using Mobile Devices to Communicate with Patients*, 8 ABA Health *e*Source, no. 2 (Oct. 2011). "Millions of cell phones and smartphones are lost or stolen every year[,]" and "approximately 22% of the total number of mobile devices produced will be lost or stolen during their lifetime, and over 50% of these will never be recovered." Ernst & Young, *Bring Your Own Device: Security and Risk Considerations for Your Mobile Device Program*, Insights on Governance, Risk & Compliance 4 (Sept. 2013). And while the security of the devices themselves is critical, best practices also require a variety of additional protections be implemented with respect to the device's operating system, applications, and other content on the device itself. These protections are critical whether the device is locked or unlocked, because the data stored on mobile devices is regularly targeted by social engineering attacks, malware, and other web and network-based attacks. FCC, *Cyber Security Planning Guide*, at MD–1. As the Government Accountability Office told Congress several years ago, "[t]hreats to the security of mobile devices and the information they store and process have been increasing significantly." U.S. Gov't Accountability Office ("GAO"), GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*, at "Highlights" page (2012). Between July 2011 and May 2012 alone, the number of malware attacks on mobile devices jumped *185%*. *Id.*; *see id.* at 11–14 ("Attacks on Mobile

Devices Are Increasing"); *see also* Paul Ruggiero & Jon Foote, United States Computer Emergency Readiness Team, *Cyber Threats to Mobile Phones* (2011).

In light of these risks, the public is demanding stronger and stronger privacy and security protections. *See*, *e.g.*, Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission ("FTC"), *Beyond Cookies: Privacy Lessons for Online Advertising*, AdExchanger Industry Preview 2015 (Jan. 21, 2015) ("consumer awareness and demand for privacy continues to grow" and there is "even consumer reluctance to engage fully in the marketplace as a result" of these concerns). In response, companies have taken a variety of measures to protect privacy and security. Software companies have been at the forefront, developing security tools that are sold directly to consumers or other businesses. *See*, *e.g.*, Heidi Hoopes, *Apps to Easily Encrypt Your Text Messaging and Mobile Calls*, Gizmag (Sept. 27, 2014); Brad Chacos, *Here's How to Best Secure Your Data Now That the NSA Can Crack Almost Any Encryption*, PC World (Sept. 6, 2013).

The current federal regulatory framework not just tolerates but actively encourages that approach. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, No. 15-mc-1902, --- F. Supp. 3d ---, 2016 WL 783565, at *19 n.29 (E.D.N.Y. Feb. 29, 2016) ("Not only has Apple done nothing wrong in marketing devices with such strong data security features, it has exercised a freedom that Congress explicitly deemed appropriate in balancing the needs of law enforcement against the interests of private industry."). The FTC, for example, has repeatedly urged app developers to take privacy and security seriously. *See*, *e.g.*, FTC, *What's the Deal? An FTC Study on Mobile Shopping Apps* 6 n.16 (2014) (hereinafter "FTC Study") ("reiterat[ing] [the FTC's] call for [app] companies to practice 'Privacy by Design' and to offer consumers simplified choices over how their data is handled") (citing additional FTC guidance). Companies do so, and regularly compete over the efficacy of the technologies they have developed.[2] Their innovations in this space benefit not just the public but also the federal government. *See*, *e.g*., Tomio Geron, *Something Ventured: Uncle Sam Is Staking Start-Ups*, VentureWire (Mar. 12, 2008) (discussing the federal government's funding of, and purchases from, IronKey, which develops encryption and other data security products). As discussed below, the Government's demands in this case would severely compromise the ability of software companies to meet the public's demands, as well as the demands of other federal government agencies, for secure data storage and communications.

ARGUMENT

The Government's demands would impose an unprecedented and extraordinary burden on numerous industry participants. If changes to the policy framework governing the mobile economy's vital technologies need to be made, such changes should come from Congress—not by way of an ad hoc process based on a misapplication of a 227-year-old law. As Magistrate Judge Orenstein of the U.S. District Court for the Eastern District of New York held earlier this week in rejecting a similar attempt by the Government to use the All Writs Act, "the relief the government seeks is unavailable because Congress has considered legislation that would achieve the same result but has not adopted it." *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *1; *see id*. at *17 (recognizing that the type of Government application for assistance here "fails to satisfy the [All Writs Act's] statutory requirements"). Moreover, in the

[2] This is to be expected because of how consumers value privacy and security. *See* Scott J. Savage & Donald M. Waldman, *The Value of Online Privacy* (Univ. of Colo. at Boulder, Working Paper No. 13-02, 2013) (determining that "privacy permissions are . . . important characteristics a consumer considers when purchasing a smartphone app" and that "[t]he representative consumer is willing to make a one-time payment of $2.28 to conceal their online browser history, $4.05 to conceal their list of contacts, $1.19 to conceal their location, $1.75 to conceal their phone's identification number, and $3.58 to conceal the contents of their text messages").

course of rejecting the Government's request there, the court recognized that the request was *less* burdensome than the one pending before this Court. *See id.* at *1 n.3 (the request there involved Apple's iOS7, not "later versions" of Apple's operating system, which present "important differences . . . in terms of the difficulty of bypassing passcode security"); *id.* at *10 n.14 ("more intrusive relief . . . is precisely what the government seeks in the *California* action," *i.e.*, the case pending here); *id.* at *22 ("[T]he government continues to seek orders compelling Apple's assistance in bypassing the passcode security of more recent models and operating systems, notwithstanding the fact that such requests are more burdensome than the one pending here.").

I. THE BURDEN THE GOVERNMENT SEEKS TO IMPOSE IS UNPRECEDENTED.

The "assistance" that the Government has compelled through the All Writs Act here is unprecedented and extraordinary. By the Government's account, the All Writs Act empowers the federal government to compel companies to write software to assist law enforcement, simply because those companies "write[ ] software code as part of [their] regular business." Gov't's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents at 15 (C.D. Cal. Feb. 16, 2016) [ECF Docket Entry 18] (hereinafter "*Ex Parte* Application"); *id.* ("the order in this case requires Apple to provide modified software"). The Government contends that this power over a third party, which has not engaged in any wrongful conduct, is incident to a "warrant authorizing the search" of property used by an accused criminal and the property owner's "consent." *Id.* at 1. The notion that the All Writs Act permits this remedy—which more closely resembles a mandatory injunction imposed against a defendant found liable for causing significant harm or the type of structural relief found in a consent decree—is incredible. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *20–24 (rejecting the Government's request for All Writs Act relief, and explaining that the assistance the Government attempted to compel has no parallel in and "is irreconcilable with," *id*. at *23, the line of cases upon which the Government also relies here).

Moreover, nothing in the Government's argument limits this construction of the All Writs Act to the device and operating system at issue here; to a particular type of privacy measure used to protect the device, its operating system, its applications or its data; to the type of software company (multi-national with extraordinary resources) whose assistance is being conscripted; or to the type of crime (terrorism and mass murder) that gave rise to the search warrant with which the third party is now compelled to assist. Nor are any of the Government's arguments logically capable of doing so. *See generally id*. at *23–24. The interpretation of the All Writs Act that would allow the Government to compel Apple to write software to avoid the security measures currently in place on the locked phone in question would similarly allow the Government to compel any software company of any size to rewrite, alter, or destroy their software programs if that would assist the Government in an investigation. *See id*. at *13 ("[T]he implications of the government's position are so far-reaching—both in terms of what it would allow today and what it implies about Congressional intent in 1789—as to produce impermissibly absurd results.") (citation omitted); *id*. at *24 ("Nothing in the government's arguments suggests *any principled limit* on how far a court may go in requiring a person or company to violate the most deeply-rooted values to provide assistance to the government the court deems necessary.") (emphasis added).

Because the number of players in the computer technology industry (and, more specifically, the mobile economy, *see State of the App Economy*, *supra*, at 2–4, 8–10) is large and increasing, and because many of those industry participants use proprietary methods both to protect data privacy *and* "write[ ] software code," *Ex Parte* Application at 15, the Government's ability to commandeer a third party to alter an operating system or to write new software in the interest of law enforcement objectives has enormous repercussions. The form of "assistance" the Government has conscripted Apple to provide here would require massive expenditures of time and resources from *any* industry player, and it would be exceptionally onerous for the small companies that constitute the majority of ACT's members and that are the heart of the mobile economy. The extent, if any, to which the thousands of participants in the App Economy should be enlisted to aid the Government in criminal investigations in such a manner was not resolved by Congress in 1789 when it passed the All Writs Act, and the courts should allow Congress to address the issue now rather than fashioning what would be in effect a common law solution to a significant matter of public policy. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *27 ("It would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate [relevant to such motions to compel assistance], and ended it, in 1789.").

A. The All Writs Act Does Not Support The Type Of Burdensome Assistance Compelled Here.

"The All Writs Act provides that federal courts 'may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.'" *In re Cty. of Orange*, 784 F.3d 520, 526 (9th Cir. 2015) (quoting 28 U.S.C. § 1651). The scope of the Act may "extend[ ], under appropriate circumstances, to persons who [are] not parties to the original action" and potentially "encompasses even those who have not taken any affirmative action to hinder justice." *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977) (citation omitted). As summarized by the Ninth Circuit, "[i]n *New York Telephone*, the Supreme Court held that the All Writs Act empowered the district court to order a third party telephone company to provide facilities it regularly used for its own purposes to assist the FBI to conduct a search." *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). Such an order, according to the Supreme Court, was "authorized by the All Writs Act and was consistent with the intent of Congress." *New York Tel. Co.*, 434 U.S. at 172. The Supreme Court, however, made clear that "the power of federal courts to impose duties upon third parties is not without limits[,]" and that "unreasonable burdens may not be imposed." *Id.*

The All Writs Act, "read with the *New York Telephone* gloss, permits the district court, in aid of a valid warrant, to order a third party to provide *nonburdensome* technical assistance to law enforcement officers." *Plum Creek*, 608 F.2d at 1289 (emphasis added). In that way, the All Writs Act can serve as an interstitial, gap-filling tool. But it is also important to bear in mind what the All Writs Act does *not do*. The statute "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 . . . inspectors." *Id.* "It does not authorize a court to order a party to bear risks not otherwise demanded by law, or to aid the government in conducting a more efficient investigation, when other forms are available." *Id.* at 1289–90. It does not constitute "a grant of plenary power to the federal courts." *Id.* at 1289; *see In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *17–18, *20–24 (discussing *New York Telephone*).

The Government's position here flaunts those principles. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *1, *5–17. The Government seeks a power that extends far beyond any previously recognized under the All Writs Act. Notably, the Government cannot point to a *single* case under the All Writs Act (or otherwise), in which a court compelled a third party to build software, let alone to restructure a business, in order to assist in a criminal investigation. *See*, *e.g.*, *Ex Parte* Application at 14–16. There is a good reason for this: Such a power is utterly unprecedented, and it is all the more extraordinary here where the Government invokes this power against a third party—a third party who, moreover, has acted *within* the carefully-constructed privacy frameworks established by Congress.[3]

"The growth of electronic communications has stimulated Congress to enact statutes that provide both access to information heretofore unavailable for law enforcement purposes and, at the same time, protect users of such communication services from intrusion that Congress deems unwarranted." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 306 (3d Cir. 2010); *see generally In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *5–7, *8–17 (discussing existing legislation and legislation Congress has chosen not to enact); Apple's Mot. at 8–10, 16–18 (discussing statutes relevant here).[4] This framework struck an important balance: For example, "[f]inding that 'new and emerging telecommunications technologies pose problems for law enforcement,'" Congress sought "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies . . . while protecting the privacy of communications and *without impeding the introduction of new technologies, features, and services*[.]" *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 454 (D.C. Cir. 2000) (emphasis added) (citation omit-

[3] Notwithstanding the Government's statement that "providers of electronic communications services and remote computing services are sometimes required to write code in order to gather information in response to subpoenas or other process[,]" *Ex Parte* Application at 15, the Government cannot point to a single instance where the *All Writs Act* has imposed the requirement. That Congress may have *legislated* such requirements in other contexts does not strengthen the Government's case here, *see generally In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *9–12; it instead shows why the Government's position must be rejected.

[4] As the Third Circuit has summarized, "[t]he Stored Communications Act . . . , was enacted in 1986 as Title II of the Electronic Communications Privacy Act of 1986 . . . , Pub.L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701–2711 (2010)), which amended the Omnibus Crime Control and Safe Streets Act of 1968, . . . Pub.L. No. 90-351, 82 Stat. 197 (1968). In 1994, Congress enacted the Communications Assistance for Law Enforcement Act [CALEA], Pub.L. No. 103-414, 108 Stat. 4279, 4292 (1994) (codified in relevant part at 18 U.S.C. § 2703 (2010)), in part to amend the [Stored Communications Act]." *In re Application*, 620 F.3d at 306 (footnote omitted).

ted).

But the Government now seeks to do an end-run around the existing framework—and stands to demolish the significant reliance interests associated with it—and, instead, arrogate to itself new powers that impose extraordinary burdens. "The obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business[.]" *In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1145 (9th Cir. 2003). App developers have taken privacy and security seriously, and built entire business models based on delivering information security to their customers. Now, the Government (by which we mean specifically the law enforcement arm of the Executive, not the federal government more broadly) wants to weaken data protection. And weaker data protection is bad for business, bad for innovation, and ultimately bad for consumers. (By contrast, it would be a boon to hackers, cyberterrorists and unfriendly or rogue governments.) Moreover, when companies have been told by legislators, policy-setting agencies and consumers that they should aspire to create the strongest protections possible, and then certain actors in the Executive Branch seek to undo those protections after the fact—without prior notice, let alone comment and debate—it imposes unanticipated harms on developers while disrupting the marketplace, discouraging innovation, and failing to account for the full range of relevant economic and consumer interests. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *26–27.

Indeed, the Government's distortion and misapplication of *New York Telephone* makes Justice Stevens's dissent in that case appear prophetic. *See New York Tel. Co.*, 434 U.S. at 178–91 (Stevens, J., dissenting in part). The dissent suggested that while the relatively mild burden imposed in *New York Telephone* might not be "particularly offensive," the order at issue in that case nevertheless was "deeply troubling as a portent of . . . powers that future courts may find lurking in the arcane language of . . . the All Writs Act." *Id*. Justice Stevens might well have been speaking of the Government's position in this case.[5]

B. The Government Misapprehends The Extraordinary Burdens, Particularly On Small Companies, That Compelled Assistance Of This Type Imposes.

The Government's arguments against the existence of an unreasonable burden not only are unsupported by any case law, but they also misconstrue the burdens at issue. At bottom, the Government's position rests on fallacies. *See Ex Parte Application* at 15. That one can build software that fulfills a particular function in the first instance does not mean that one can undo it without creating significant harms. The risks associated with such revisions are especially severe where, as here, the modifications need to occur at the operating system level of the code, because the operating system affects all applications that run on and data stored on the device and therefore can create cascading problems throughout. *See*, *e.g*., Apple, *Unauthorized Modification of iOS Can Cause Security Vulnerabilities, Instability, Shortened Battery Life, and Other Issues* (Sept. 22, 2015). Indeed, the Government's position borders on the absurd in the context of software development. Not only are the burdens imposed extraordinary (*i.e*., diverting resources from company's actual business to being a tool

[5] As Justice Stevens observed, the type of power the Government seeks here *might* find a certain historical parallel in the common law "writ of assistance." *New York Tel. Co*., 434 U.S. at 180. "The writ of assistance . . . took its name from its command that all peace officers and any other persons who were present 'be assisting' in the performance of the search." Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 561 n.18 (1999). Such writs "commanded 'all officers and subjects of the Crown to assist in their execution,' and were not returnable after execution, but rather served as continuous authority during the lifetime of the reigning sovereign." *New York Tel. Co*., 434 U.S. at 180 n.3 (quoting N. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* 53–54 (1937)). But "[t]he use of that writ by the judges appointed by King George III was one British practice that the Revolution was specifically intended to terminate." *Id*. at 190; *see Brower v. Cty. of Inyo*, 489 U.S. 593, 596 (1989) (identifying "writs of assistance" as "the principal grievance against which the Fourth Amendment was directed").

of government),[6] but the goals the Government seeks to achieve are far from assured. As any computer user knows, many software patches, which are far more basic than what the Government seeks to compel here, fail to fix problems, make other things worse, or simply necessitate more patches.

Additionally, although Apple faces extraordinary burdens here, *see* Declaration of Erik Neuenschwander in Support of Apple's Mot. (Feb. 25, 2016), the burdens likely would be far weightier for a smaller or startup software company conscripted to develop software to assist a Government investigation. Put simply, the small businesses who comprise the majority of ACT's 5,000-plus members do not have the personnel or the resources to effectuate the type of new software development that the Government compelled here. *See id.* ¶¶ 3, 21–22 (testifying that "between six and ten Apple engineers and employees" would be required). The logic set forth by the Government in obtaining relief under the All Writs Act, however, lacks any principled stopping point: *Any* app developer might generate and apply privacy and security protections that neither the developer nor the Government could crack.[7]

Moreover, the burdens associated with the sort of assistance compelled here go well beyond writing software. For one thing, not only must a company *write* the new software, its personnel—once conscripted as quasi-forensic scientists developing and testing methods to support a prosecution—likely will be haled into courts around the country to *testify* about it as well. *See generally Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 310 (2009) (forensic reports available for use at trial are "testimonial

[6] *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *20 (rejecting Government's argument that assistance it sought to compel would not impose unreasonable burdens, stating "[t]he salient points that the Court highlighted as the basis for finding a lack of unreasonable burdens in *N.Y. Tel. Co.* are virtually all absent here," notwithstanding as noted *supra* at 6, the burdens there were less than in this case).

[7] The app industry has been marked by some of the most innovative content being developed by small startups, which has directly led to larger industry players purchasing those small companies or their technologies. *See*, *e.g.*, Ivana Kottasova, *Zuckerberg Goes Shopping: Facebook's Top 10 Purchases*, CNN (Mar. 26, 2014).

statements" and a certifying analyst is a "'witness[ ]' for purposes of the Sixth Amendment").

Irrespective of whether the conscripted employees trigger a defendant's Confrontation Clause protections, a necessary incident to the compelled assistance is that a company's proprietary software used to incriminate the criminal defendant will become discoverable by the criminal defendant and by his or her experts. As a result, those experts may attempt to attack the reliability of the recovered data and the methods used to obtain it. This, in turn, likely will be subject to further court proceedings as the experts' data-recovery methodology is questioned and passed on by the trial court in its gate-keeping role. Even assuming that the "strong presumption in favor of access to court records," *Foltz v. State Farm Mut. Auto. Ins. Co.*, 331 F.3d 1122, 1135 (9th Cir. 2003), is overcome and that robust protective orders remain in place throughout this process, some disclosure of the software company's proprietary methods would be inherent to this process. Consistent with this, companies, consumers and the United States Government itself reasonably should fear that, once the privacy protections are compromised for one purpose, they will more readily be compromised by hackers, criminals, and foreign governments from which they have attempted to shield such information.

Although one cannot predict with absolute certainty the full range of second-order effects resulting from the Government's use of the All Writs Act in this manner, there is no question that even the mere prospect of these extraordinary burdens will chill innovation and deter companies and individuals from entering this important space.[8] Technology development will be compromised, perhaps radically so, in an

[8] Moreover, the Government's position may have adverse consequences even with respect to those actors that choose to remain in the privacy and security marketplace. Specifically, because the magnitude of the burdens imposed often will vary in proportion to the security of the measures in place, *see In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *22, the Government's proposed use of the All Writs Act would perversely incentivize use of measures that provide *less* privacy and security protections for businesses

(Footnote continued)

area of exceptional importance to consumers and the broader economy—despite that the federal government's other arms, as noted, have encouraged and in some cases required companies to focus on and strengthen data privacy and security. The unprecedented order the Government seeks is not authorized by the All Writs Act; it would impose an extraordinary and unreasonable burden both on Apple and on thousands of other entities across the App Economy.

C. These Burdens Cannot Be Cabined To This Particular Case.

Finally, it is important to understand how broadly applicable the powers sought by the Government would be, in practice. Notwithstanding the Government's attempts to emphasize the specific facts of this case, *see Ex Parte* Application at 1–4, 16–17, there is nothing in the Government's argument that provides a principled stopping point that would limit the assistance sought to cases such as this one. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *13, *22–24. The Government's argument regarding the lawfulness of this Court's order does not, for example, carefully weigh the specifics of its interest in investigating and combating terrorism against the specifics of the burden imposed.[9] Rather, it focuses only on the supposed lack of a burden on Apple, which is based on reasoning that, as explained, would apply to any company that writes software. The Government does this, presumably, because it does not actually *want* an order that would apply "'Just this once.'" Apple's Mot. at 3.

For example, as recently disclosed in the Eastern District of New York case discussed throughout this brief, the federal government has sought similar orders in-

and consumers. This would undermine the government's broader aims of fostering increased security. *See*, *e.g.*, FTC Study, *supra* at 4.

[9] The Government's presumption is that where a company's technology is implicated in a government investigation, *see Ex Parte* Application at 13–14, and where a company's technology provides some barrier to fully effectuating a warrant, *id.* at 16–17—conditions that often will be met where data privacy is at issue—a company can be compelled to write software relevant to the same technological subject matter, *id.* at 14–16.

volving twelve other devices manufactured by Apple alone. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, 2016 WL 783565, at *22; *see also* Julia Angwin, *What's Really at Stake in the Apple Encryption Debate*, ProPublica (Feb. 24, 2016). Moreover, as Manhattan District Attorney Cyrus Vance has stated, this issue implicates not just federal investigations, but "virtually all criminal investigations, the overwhelming majority of which are handled by state and local law enforcement." Cyrus R. Vance Jr., *No Smartphone Lies Beyond the Reach of a Judicial Search Warrant*, N.Y. Times (Feb. 18, 2016). Vance's office alone "has 175 iPhones it can't open." Alyssa Newcomb, *New York DA Says He Can't Access 175 iPhones From Criminal Cases Due to Encryption*, ABC News (Feb. 18, 2016).

The Government's position converts every criminal investigation into an opportunity to enlist the aid of software companies. But the All Writs Act is a gap-filling tool, not a license for the federal courts to regulate a critical function of a rapidly growing $120 billion industry through the common law. The kinds of trade-offs between national security and data security that the Government asks this Court to make require the gathering of information and the reconciliation of competing national policy goals that Congress should address. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, 2016 WL 783565, at *8–17, *26–27.

II. IF THE GOVERNMENT WANTS THESE NEW TOOLS, IT SHOULD SEEK NEW LEGISLATION, NOT USE THE ALL WRITS ACT

There is no doubt that tensions and competing interests exist between law enforcement's interests and the broader interest of ensuring data privacy. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court*, 2016 WL 783565, at *26. To address the sensitive balancing of these considerations, however, the answer is not to contort the All Writs Act and *New York Telephone* beyond recognition. If a change needs to be made to the manner in which the interests at issue here are weighed, it should be made by Congress. "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." *Pennsylvania Bureau of Correction v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985). The Act, in other words, is a narrow tool designed to fill in statutory gaps. Although it "empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *Id.*; *see In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *5–17; Apple's Mot. at 14–19.

"The All Writs Act is not a grant of plenary power to the federal courts," nor is it a font of "wide-ranging inherent powers" pursuant to which a court may "impose a duty on a private party when Congress has failed to impose one." *Plum Creek*, 608 F.2d at 1289–90. "To so rule would be to usurp the legislative function and to improperly extend the limited federal court jurisdiction." *Id.*

The Government invites this Court to conclude that it somehow would be "consistent with the intent of Congress," *New York Tel. Co.*, 434 U.S. at 172, for the All Writs Act to give courts and prosecutors the power to effect cataclysmic change across a $120 billion industry, disrupting many settled expectations and threatening critical consumer privacy interests in the process. But Congress "does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes." *Whitman v. Am. Trucking Assns.*, 531 U.S. 457, 468 (2001). Still less should such a change be based on the mere *possibility* that Congress may have "failed to consider" the type of compelled action sought here. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, No. 1:15-mc-1902, 2015 WL 5920207, at *1 (E.D.N.Y. Oct. 9, 2015). This is particularly so when Congress has legislated within this very field and chose not to go further. *See* discussion *supra* at I.A; *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *19 n.29 ("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 *10 n.13; Apple's Mot. at 8–10, 16–18.

If it wished to do so, Congress could legislate against the forms of information security that the Government is seeking to bypass. *See*, *e.g*., *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *12.[10] The issue clearly has not escaped Congress's attention. Just yesterday—on March 1, 2016—the House Judiciary Committee held a hearing entitled *The Encryption Tightrope: Balancing Americans' Security and Privacy*. H. Comm. on the Judiciary, 114th Cong. (2016). Here, the "tightrope" should be Congress's to walk, not this Court's. If the Government needs new law-enforcement tools, and if those needs outweigh Americans' vital privacy and security interests, then that decision should be debated and properly addressed to Congress, not to this Court: "Congress has the prerogative to determine the exact right response—choosing the policy fix, among many conceivable ones, that will optimally serve the public interest." *Kimble v. Marvel Entm't, LLC*, 135 S. Ct. 2401, 2414 (2015). With new legislation, companies could assess the risks and burdens *ex ante*, and they could ensure that their voices are heard, and that *all* the relevant factors are considered. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued*

[10] Of course, it is not clear whether such an action would have the support of the American people. *See, e.g*., Jim Finkle, *Solid Support for Apple in iPhone Encryption Fight: Poll*, Reuters (Feb. 24, 2016) ("Forty-six percent of respondents said they agreed with Apple's position, 35 percent said they disagreed and 20 percent said they did not know, according to poll results released on Wednesday. Other questions in the poll showed that a majority of Americans do not want the government to have access to their phone and Internet communications, even if it is done in the name of stopping terror attacks.").

by the Court, 2016 WL 783565, at *26–27. The All Writs Act should not be used to effect dramatic change that fails to account for the full range of relevant interests, disrupts settled expectations, and imposes considerable harms on one of the country's most important economic engines.

CONCLUSION

For the foregoing reasons, *amicus curiae* ACT urges the Court to grant Apple's Motion to Vacate the Order Compelling Apple Inc. to Assist Agents in Search.

Dated: March 2, 2016

SIDLEY AUSTIN LLP

By: ______________________

Mark E. Haddad
Eamon P. Joyce
Nicholas M. McLean
Attorneys for *Amicus Curiae* ACT | The App Association