

**1:15-mc-01902-JO** Order requiring Apple, Inc. to assist in the execution of a search warrant issued by the court et al

James Orenstein, presiding

**Date filed:** 10/08/2015

**Date of last filing:** 10/20/2015

Filed & Entered: 10/20/2015

**Full docket text:**

ORDER re [11] Notice(Other) filed by Apple Inc.: In inviting Apple, Inc. ("Apple") to submit its views on the feasibility and burdensomeness of the government's request, I did not intend to limit its submission to those matters, but rather to focus its attention on particular factual questions. I therefore respectfully invite Apple to supplement its submission by addressing the legal question before the court; namely, whether the All Writs Act empowers the court to compel Apple to provide the technical assistance the government seeks. If Apple can do so in advance of the hearing on October 22, 2015 (at which I would benefit from Apple's participation and availability to answer questions, should they arise, even if Apple does not affirmatively wish to present an oral argument), I request that it do so; otherwise, I respectfully direct the government and Apple to submit a proposed revised schedule. Ordered by Magistrate Judge James Orenstein on 10/20/2015. (Orenstein, James)

Filed & Entered: 10/20/2015

**Full docket text:**

ORDER denying [10] Motion for Leave to File -- I am grateful to the proposed *amici* for their proffered assistance, but I conclude that it is unnecessary. Although the government filed the pending motion for relief under the All Writs Act *ex parte*, the entity it seeks to have the court compel has been afforded an opportunity to vindicate its interests by submitting a brief. While the proposed *amici*, among many others, may have a fresh perspective on a broader policy debate surrounding the instant that the briefs I have already solicited may not fully address, the sole legal issue before the court is a narrow one that directly affects only the government and Apple, Inc. and that they are fully capable of exploring thoroughly in their submissions. I therefore exercise my discretion to deny the motion. *Cf. United States v. Yaroshenko*, 86 F. Supp. 3d 289, 291 (S.D.N.Y. 2015). Ordered by Magistrate Judge James Orenstein on 10/20/2015. (Orenstein, James)

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

IN RE ORDER REQUIRING APPLE INC. TO  
ASSIST IN THE EXECUTION OF A SEARCH  
WARRANT ISSUED BY THIS COURT

No. 15 MISC 1902 (JO)

**APPLE INC.'S RESPONSE TO  
COURT'S OCTOBER 9, 2015 MEMORANDUM AND ORDER**

## INTRODUCTION

This Court asked for Apple’s views on whether the assistance the government seeks from Apple is technically feasible and, if so, whether compliance with the proposed order would be unduly burdensome. But the Court has also raised an important question of first impression—does the government have the ability to use the All Writs Act to compel a provider of consumer electronic devices like Apple to assist law enforcement in its investigative efforts? This question is particularly timely because social awareness of issues relating to privacy and security, and the authority of government to access data is at an all-time high. And public expectations about the obligations of companies like Apple to minimize government access within the bounds of the law have changed dramatically. Apple acknowledges the basis for this Court’s concern that the All Writs Act may not be sufficient authority to require a device manufacturer like Apple to take possession of a device in the government’s custody and perform expert forensic services on that device<sup>1</sup> but, as requested by the Court, Apple will limit its response to the topics of feasibility and burden.<sup>2</sup>

## FEASIBILITY AND BURDEN OF THE GOVERNMENT’S REQUEST

In most cases now and in the future, the government’s requested order would be substantially burdensome, as it would be impossible to perform. For devices running iOS 8 or higher, Apple would not have the technical ability to do what the government requests—take possession of a password protected device from the government and extract unencrypted user

---

<sup>1</sup> The All Writs Act may not apply here because, among other reasons, the bounds of mandatory law enforcement assistance have already been drawn by the Communications Assistance for Law Enforcement Act (CALEA) and because Apple does not own or control the device in question.

<sup>2</sup> Apple is not requesting oral argument.

data from that device for the government. Among the security features in iOS 8 is a feature that prevents anyone without the device's passcode from accessing the device's encrypted data. This includes Apple.

A more detailed explanation of Apple's security features for iOS 8 and higher can be found in Apple's iOS Security Guide. *See, e.g., iOS Security—White Paper*, Apple Inc. (September 2015), [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf) (last visited Oct. 19, 2015). But at a high level, as relevant here, each Apple device includes both hardware and software security features. For example, each device is provisioned during fabrication with its own Unique ID ("UID") that is not accessible to other parts of the system and is not known to Apple. *Id.* at 10-12. When a user sets up a device passcode, that passcode becomes entangled with the device's UID. *Id.* The passcode thus becomes part of the key-management protections for files encrypted with certain classes of protection. *Id.* The stronger the user passcode is, the stronger the encryption becomes. In iOS 8, the default class of protection changed, and the encryption keys used for the vast majority of files stored on devices now are protected with a key derived from the user-chosen passcode. *Id.* The end-result is that a person must know the passcode to decrypt the majority of the data on the device. This combination of hardware and software security features helps protect users from attackers if Apple's servers are compromised or if the user no longer has physical possession of his or her device. As measured by Apple's App Store, as of October 5, 2015, 90% of Apple's devices are using iOS 8 or higher. *See Support: App Store*, Apple Developer, <https://developer.apple.com/support/app-store/> (last visited Oct. 19, 2015).

Here, however, the case involves an Apple device running a version of iOS 7. Such operating system versions are becoming rare as they comprise less than 10% of the devices in

the U.S. For these devices, Apple has the technical ability to extract certain categories of unencrypted data from a passcode locked iOS device.<sup>3</sup> Whether the extraction can be performed successfully depends on the device itself, and whether it is in good working order. As a general matter, however, certain user-generated active files on an iOS device that are contained in Apple's native apps can be extracted. Apple cannot, however, extract email, calendar entries, or any third-party app data.

Apple has not inspected the device that is the subject of the government's application so Apple cannot say with certainty that it can extract the requested data. Nor can Apple say with certainty what the burden would be to perform such an extraction assuming it is possible. But the act of extracting data from a single device in good working order, running an operating system earlier than iOS 8, would not likely place a substantial financial or resource burden on Apple by itself. But it is not a matter of simply taking receipt of the device and plugging it into a computer. Each extraction diverts man hours and hardware and software from Apple's normal business operations. And, of course, this burden increases as the number of government requests increases.

Moreover, as the Court recognized in its Memorandum and Order, there may be burdens to Apple beyond "the physical demands and immediate monetary costs of compliance." Oct. 9, 2015 Mem. and Order at 9 (ECF No. 2). The first is the inevitable testimonial demands that will follow such extraction. Once Apple engineers participate in the process, they may be required to testify at trial. *See, e.g., U.S. v. Cameron*, 699 F.3d 621, 643-44, 49 (1st Cir. 2012) (holding that

---

<sup>3</sup> Apple has previously been ordered to extract data from devices running iOS 7 or earlier and has performed such extractions. These orders generally come in the body of search warrants and contain specific language to avoid confusion over the scope and legitimacy of the demand on Apple. This case marks the first time a judge has questioned the authority of the All Writs Act to grant supplemental orders to accompany such warrants and asked Apple for its views on the feasibility and burden associated with such an order before issuing it.

because child pornography reports generated by Internet provider were testimonial, the reports “should not have been admitted without giving [defendant] the opportunity to cross-examine the [provider] employees who prepared the [reports].”) Again, in a single case, that burden may be manageable, but on any significant scale it can be demanding and personnel-intensive. This is not a case where Apple engineers are fact witnesses, required to testify when called. Their involvement in any proceedings would be solely due to their mandated service under the proposed order.

Second, public sensitivity to issues regarding digital privacy and security is at an unprecedented level. This is true not only with respect to illegal hacking by criminals but also in the area of government access—both disclosed and covert. Apple has taken a leadership role in the protection of its customers’ personal data against any form of improper access. Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand. This reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue.

### **CONCLUSION**

The questions this Court raised in its Memorandum and Order are both vital and timely. Application of the All Writs Act in this case imposes a real burden on Apple—commercial and reputational. Should the Court determine that the law does not support the government’s reliance on the All Writs Act for the reasons the Court identified, Apple respectfully requests that the Court deny the government’s application for an order requiring Apple to perform extraction services on the Apple-manufactured device in the government’s custody.

Dated: October 19, 2015

Respectfully submitted,

/s/ Ken Dreifach

Ken Dreifach (Bar No. KD4816)

ZwillGen PLLC

232 Madison Avenue

New York, NY 10016

(646) 362-5590

Marc Zwillinger (*pro hac vice*)

Jeffrey Landis (*pro hac vice*)

ZwillGen PLLC

1900 M Street, NW, Suite 250

Washington, DC 20036

(202) 296-3585

*Counsel for Apple Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on October 19, 2015, the foregoing document was filed with the Clerk of the Court and served in accordance with the Federal Rules of Civil Procedure, the Eastern District's Local Rules, and the Eastern District's Rules on Electronic Service upon the following parties and participants:

Lauren Howard Elbert  
Assistant United States Attorney  
Eastern District of New York  
271 Cadman Plaza East  
Brooklyn, NY 11201  
(718) 254-7577

/s/ Jeffrey Landis  
Jeffrey Landis (*pro hac vice*)  
ZwillGen PLLC  
1900 M Street, NW, Suite 250  
Washington, DC 20036  
(202) 296-3585



**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

IN RE ORDER REQUIRING APPLE, INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT.

No. 1:15-mc-01902-JO

**MOTION FOR LEAVE TO FILE BRIEF OF *AMICI CURIAE*  
AMERICAN CIVIL LIBERTIES UNION, NEW YORK CIVIL LIBERTIES UNION,  
ELECTRONIC FRONTIER FOUNDATION, AND JENNIFER GRANICK AND RIANA  
PFEFFERKORN**

Proposed *Amici Curiae* the American Civil Liberties Union, the New York Civil Liberties Union, the Electronic Frontier Foundation, and Jennifer Granick and Riana Pfefferkorn, by and through undersigned counsel, hereby move the Court for leave to file the attached Brief of *Amici Curiae* in the above-captioned case. Apple, Inc. and the United States consent to the filing of this brief.

Proposed *amici* respectfully request leave to participate in any oral argument held in this matter.

In support of this motion, proposed *amici* state the following:

1. The disposition of this case is of critical importance to Americans' privacy rights in light of evolving technologies. This case raises both statutory and constitutional questions regarding the limits of government's authority to compel private parties to assist law enforcement.

2. The government's request in this case invokes the All Writs Act in an extraordinary and unjustified way because it seeks to compel a third party device manufacturer not accused of wrongdoing to obtain and transform information for law enforcement that the third party does not possess or control. The request is not authorized by the All Writs Act because Congress has consciously withheld authority for the type of compelled assistance required here. And it would violate the Constitution, because the Fifth Amendment's protection of property and liberty safeguards individuals against conscription into government service where they do not, at the very least, possess or control the information the government seeks.

3. Proposed *amici* frequently appear as direct counsel or *amicus curiae* in cases raising similar legal issues to those here.

4. Proposed *amici* the American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts, both as direct counsel and as *amicus curiae*, in numerous cases implicating Americans' right to privacy. The ACLU and its members have long been concerned about the impact of new technologies on constitutional rights. The ACLU is particularly concerned with protecting the lawful use of strong encryption technologies, which are essential to preserving the constitutional guarantees of privacy, free expression, and anonymity in the digital age. The New York Civil Liberties Union is the New York State affiliate of the ACLU.

3. Proposed *amici* the Electronic Frontier Foundation ("EFF") is a member-supported nonprofit organization devoted to protecting civil liberties and free expression in technology, law, policy, and standards. With over 22,000 dues-paying members, EFF is a leading

voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment. EFF has campaigned both in the United States and abroad against ill-considered efforts to block, filter, or degrade access to the public Internet. EFF develops and promotes tools that help consumers and public interest groups test their broadband connections to see if their providers are interfering with the traffic to and from users' computers. EFF has been involved in promoting sound policy in the realm of cryptography and the law since the 1990s, when it represented Daniel J. Bernstein in his successful challenge to the inclusion of encryption software on the United States Munitions List. *See Bernstein v. United States*, 192 F.3d 1308 (9th Cir. 1999).

4. Proposed *amici* Jennifer Granick and Riana Pfefferkorn, joining as *amici* in their individual capacities, are the Director of Civil Liberties and the Cryptography Policy Fellow with the Stanford Center for Internet and Society, respectively. The Center for Internet and Society ("CIS") is a public interest technology law and policy program at Stanford Law School and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry.

5. Counsel for *amici curiae* states that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

Proposed *amici* respectfully request leave to file the attached brief of *amici curiae* and to participate in any oral argument held in this matter.

October 19, 2015

Respectfully Submitted,

Arthur Eisenberg  
Mariko Hirose  
New York Civil Liberties Union  
125 Broad Street, 19th Floor  
New York, NY 10004  
Tel: 212-607-3300  
aeisenberg@nyclu.org

By: /s/ Esha Bhandari

Esha Bhandari  
Alex Abdo  
American Civil Liberties Union  
Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
Tel: 212-549-2500  
ebhandari@aclu.org

Jennifer Stisa Granick (CA Bar #168423)  
Director of Civil Liberties\*  
Riana Pfefferkorn (CA Bar #266817)  
Cryptography Policy Fellow\*  
Stanford Law School  
Center for Internet and Society  
559 Nathan Abbott Way  
Stanford, CA 94305  
Tel: 650-736-8675  
jennifer@law.stanford.edu  
\* For affiliation purposes only

Andrew Crocker  
Nathan D. Cardozo  
Electronic Frontier  
Foundation  
815 Eddy Street  
San Francisco, CA 94109  
Tel: 415-436-9333  
andrew@eff.org

**CERTIFICATE OF SERVICE**

I hereby certify that on this 19th day of October, 2015, the foregoing Motion for Leave to File Brief of *Amici Curiae* American Civil Liberties Union, New York Civil Liberties Union, Electronic Frontier Foundation, and Jennifer Granick and Riana Pfefferkorn, along with its accompanying Brief of *Amici Curiae*, was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all counsel of record by operation of the Court's electronic filing system.

*/s/ Esha Bhandari*

---

Esha Bhandari

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

IN RE ORDER REQUIRING APPLE, INC.  
TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT ISSUED BY THIS  
COURT.

No. 1:15-mc-01902-JO

**BRIEF OF *AMICI CURIAE*  
AMERICAN CIVIL LIBERTIES UNION, NEW YORK CIVIL LIBERTIES UNION,  
ELECTRONIC FRONTIER FOUNDATION, AND JENNIFER GRANICK AND RIANA  
PFEFFERKORN**

Arthur Eisenberg  
Mariko Hirose  
New York Civil Liberties Union  
125 Broad Street, 19th Floor  
New York, NY 10004  
Tel: 212-607-3300  
aeisenberg@nyclu.org

Esha Bhandari  
Alex Abdo  
American Civil Liberties Union  
Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
Tel: 212-549-2500  
ebhandari@aclu.org

Jennifer Stisa Granick (CA Bar #168423)  
Director of Civil Liberties\*  
Riana Pfefferkorn (CA Bar #266817)  
Cryptography Policy Fellow\*  
Stanford Law School  
Center for Internet and Society  
559 Nathan Abbott Way  
Stanford, CA 94305  
Tel: 650-736-8675  
jennifer@law.stanford.edu

Andrew Crocker  
Nathan D. Cardozo  
Electronic Frontier  
Foundation  
815 Eddy Street  
San Francisco, CA 94109  
Tel: 415-436-9333  
andrew@eff.org

\* For affiliation purposes only

**TABLE OF CONTENTS**

TABLE OF AUTHORITIES .....ii

SUMMARY OF ARGUMENT .....2

BACKGROUND .....3

ARGUMENT .....3

    I.    The All Writs Act does not authorize the order the government seeks. ....3

        A.    The order the government seeks exceeds the bounds of the All Writs Act, because the authority to force a third party to decrypt a device does not stem from the court’s authority to issue a warrant. ....4

        B.    The All Writs Act does not confer authority that Congress has consciously withheld. ....6

    II.   It would be unconstitutional to conscript Apple into governmental service to assist in gaining access to information that Apple does not possess or control. ....10

CONCLUSION.....18

**TABLE OF AUTHORITIES**

**Cases**

*Application of the U.S.*, 427 F.2d 639 (9th Cir. 1970)..... 9

*Application of U.S. for an Order Authorizing an In-Progress Trace of Wire  
Commc’ns over Tel. Facilities*, 616 F.2d 1122 (9th Cir. 1980)..... 12, 15

*Ass’n for Retarded Citizens of Conn., Inc. v. Thorne*, 30 F.3d 367, 370 (2d Cir.  
1994)..... 5

*Bernstein v. United States*, 192 F.3d 1308 (9th Cir. 1999)..... 1

*Clark v. Martinez*, 543 U.S. 371 (2005) ..... 11

*Glosband v. Watts Detective Agency, Inc.*, 21 B.R. 963 (D. Mass. 1981)..... 12

*In re Application of the U.S. for an Order Authorizing Disclosure of Location  
Information of a Specified Wireless Tel.*, 849 F. Supp. 2d 526 (D. Md. 2011) ..... 9

*In re Application of the United States for an Order Authorizing the Use of a Pen  
Register*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005)..... 4

*In re Application of U.S. for an Order Directing a Provider of Commc’n Servs. to  
Provide Technical Assistance to Agents of the U.S. Drug Enforcement Admin.*,  
No. 15-1242 M, 2015 WL 5233551 (D.P.R. Aug. 27, 2015) ..... 16

*In re Application of U.S. for an Order Directing X to Provide Access to  
Videotapes*, No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003) ..... 16

*In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant  
Issued by this Court*, CR 14-90470 (N.D. Cal. June 6, 2014) ..... 14

*In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant  
Issued by this Court*, CR 14-90812 (N.D. Cal. Nov. 3, 2014)..... 14

*In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant  
Issued by this Court*, No. 1:15-mc-01902-JO, 2015 WL 5920207 (E.D.N.Y.  
Oct. 9, 2015) ..... 3, 4, 6, 7

*In re XXX, Inc.*, No. 14 Mag. 2258, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014)..... 14

*ITT Cmty. Dev. Corp. v. Barton*, 569 F.2d 1351 (5th Cir. 1978)..... 5

*Newark Morning Ledger Co. v. United States*, 507 U.S. 546 (1993)..... 12



*Application of U. S. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder & Terminating Trap*, 610 F.2d 1148 (3d Cir. 1979)..... 11, 15

*Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34 (1985)..... 4

*Soranno’s Gasco, Inc. v. Morgan*, 874 F.2d 1310 (9th Cir. 1989)..... 12

*The Company v. United States*, 349 F.3d 1132 (9th Cir. 2003)..... 16, 17

*United States v. Doe*, 537 F. Supp. 838 (E.D.N.Y. 1982) ..... 15

*United States v. Hall*, 583 F. Supp. 717 (E.D. Va. 1984)..... 15

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

**Statutes and Rules**

18 U.S.C. § 2511..... 9

18 U.S.C. § 2518..... 9, 16

18 U.S.C. § 2520..... 9

28 U.S.C. § 1651..... 3, 4

47 U.S.C. § 1001..... 7

47 U.S.C. § 1002..... 7

Fed. R. Crim. P. 41 ..... 4

**Other Authorities**

Andrea Peterson, *Congressman with Computer Science Degree: Encryption Backdoors Are “Technologically Stupid,”* Wash. Post (Apr. 30, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/04/30/congressman-with-computer-science-degree-encryption-back-doors-are-technologically-stupid> ..... 8

Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. Times (Sept. 27, 2010), <http://www.nytimes.com/2010/09/27/us/27wiretap.html> ..... 7

Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. Times (May 7, 2013), <http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html> ..... 7

Electronic Frontier Foundation, *Who Has Your Back*, <https://www EFF.org/who-has-your-back-government-data-requests-2015> (last visited Oct. 19, 2015)..... 13

Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, Wash. Post (Apr. 10, 2015), [https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff\\_story.html](https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html)..... 6

Ellen Nakashima, *WhatsApp, Most Popular Instant-Messaging Platform, to Encrypt Data for Millions*, Wash. Post (Nov. 18, 2014), [https://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6\\_story.html](https://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html) ..... 8

Letter from Yahoo! Inc. to U.S. Marshals Service (Sept. 15 2009), [http://www.wired.com/images\\_blogs/threatlevel/2009/12/yahoo-price-list-letter.pdf](http://www.wired.com/images_blogs/threatlevel/2009/12/yahoo-price-list-letter.pdf) ..... 13

Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S. Over Data Access*, N.Y. Times (Sept. 7, 2015), <http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html>. .... 6

Matthew Panzarino, *Apple’s Tim Cook Delivers Blistering Speech on Encryption, Privacy*, TechCrunch (June 2, 2015), <http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy> ..... 13

Mike McConnell, Michael Chertoff & William Lynn, Opinion, *Why the Fear Over Ubiquitous Data Encryption Is Overblown*, Wash. Post (July 28, 2015), [https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4\\_story.html](https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html) ..... 8

Nicole Perlroth & David E. Sanger, *Obama Won’t Seek Access to Encrypted User Data*, N.Y. Times (Oct. 10, 2015), <http://www.nytimes.com/2015/10/11/us/politics/obama-wont-see-access-to-encrypted-user-data.html>. .... 7

### **INTERESTS OF *AMICI CURIAE***

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation’s civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts, both as direct counsel and as *amicus curiae*, in numerous cases implicating Americans’ right to privacy. The ACLU and its members have long been concerned about the impact of new technologies on constitutional rights. The ACLU is particularly concerned with protecting the lawful use of strong encryption technologies, which are essential to preserving the constitutional guarantees of privacy, free expression, and anonymity in the digital age. The New York Civil Liberties Union is the New York State affiliate of the ACLU.

The Electronic Frontier Foundation (“EFF”) is a member-supported nonprofit organization devoted to protecting civil liberties and free expression in technology, law, policy, and standards. With over 22,000 dues-paying members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment. EFF has campaigned both in the United States and abroad against ill-considered efforts to block, filter, or degrade access to the public Internet. EFF develops and promotes tools that help consumers and public interest groups test their broadband connections to see if their providers are interfering with the traffic to and from users’ computers. EFF has been involved in promoting sound policy in the realm of cryptography and the law since the 1990s when it represented Daniel J. Bernstein in his successful challenge to the inclusion of encryption software on the United States Munitions List. *See Bernstein v. United States*, 192 F.3d 1308 (9th Cir. 1999).

Jennifer Granick and Riana Pfefferkorn, joining as *amici* in their individual capacities, are the Director of Civil Liberties and the Cryptography Policy Fellow with the Stanford Center

for Internet and Society, respectively. The Center for Internet and Society (“CIS”) is a public interest technology law and policy program at Stanford Law School and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry.

### **SUMMARY OF ARGUMENT**

The government has invoked the All Writs Act to compel Apple, Inc. to unlock and make available personal data stored on a private Apple-manufactured mobile device seized by the government. This is an extraordinary and unjustified attempt to compel a third party not accused of wrongdoing to assist the government in obtaining information that the third party neither possesses nor controls. Private parties may not be conscripted into governmental service where the party is simply the manufacturer of a device the government has seized, and where the government’s request goes beyond asking the party to turn over information within its possession, or to intercept communications passing through a medium it controls.

Regardless of whether Apple has the technical ability to provide the assistance requested here, compelling Apple to do so would be unlawful. It is not authorized by the All Writs Act because, as this Court previously noted, Congress has consciously withheld authority for the type of compelled assistance required here. And it would violate the Constitution, because the Fifth Amendment’s protection of liberty and property safeguards individuals against conscription into governmental service where they do not, at the very least, possess or control the information the government seeks. For these reasons, this Court should deny the government’s request.

## BACKGROUND

In a sealed application filed on October 8, 2015, the government asked this Court to issue an order pursuant to the All Writs Act, 28 U.S.C. § 1651, compelling Apple to “disabl[e] the security of an Apple device that the government has lawfully seized pursuant to a warrant.” Memorandum and Order, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, No. 1:15-mc-01902-JO, 2015 WL 5920207, at \*1 (E.D.N.Y. Oct. 9, 2015) (hereinafter Order). The following day, this Court issued an order that deferred ruling on the application and directed Apple to submit its views as to whether the government’s request is “technically feasible” and whether compliance would be “unduly burdensome.” *Id.*

Apple does not appear to possess the device or to possess the personal data that is stored on the device. *See* Order at \*1, \*7. Rather, the device appears to be a private mobile device that was manufactured and sold by Apple. The information the government seeks is apparently the owner’s personal data, which is stored on that device. Access to the device is apparently protected using a personal identification number or passcode selected by the owner.

## ARGUMENT

### **I. The All Writs Act does not authorize the order the government seeks.**

The All Writs Act does not authorize an order allowing the government to compel Apple to unlock, and potentially to decrypt data stored on, private devices seized by the government. This is so for at least two independent reasons. First, an order forcing a third party to decrypt a device does not stem from the court’s authority to issue a warrant. Second, even if the government’s lack of authority to compel unlocking or decryption is a gap that could be filled by the All Writs Act, Congress has consciously withheld that authority, and it would therefore be inappropriate to supply it through the All Writs Act.

**A. The order the government seeks exceeds the bounds of the All Writs Act, because the authority to force a third party to decrypt a device does not stem from the court’s authority to issue a warrant.**

The All Writs Act, 28 U.S.C. § 1651, allows a court to issue an order to effectuate a prior order authorized by a statute or other source of authority. *See United States v. New York Tel. Co.*, 434 U.S. 159, 172 (1977) (“This Court has repeatedly recognized the power of a federal court to issue such commands under the All Writs Act as may be necessary or appropriate to effectuate and prevent the frustration of *orders it has previously issued* in its exercise of jurisdiction otherwise obtained” (emphasis added)); *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 42 n.7 (1985) (courts may resort to the All Writs Act “to fill statutory interstices.”). As this Court has noted, the All Writs Act is not “a mechanism for the judiciary to give [the government] the investigative tools that Congress has not.” *In re Application of the United States for an Order Authorizing the Use of a Pen Register*, 396 F. Supp. 2d 294, 325 (E.D.N.Y. 2005).

The assistance the government seeks here exceeds the bounds of the All Writs Act, because the authority to force a third party to decrypt a device does not stem from the court’s authority to issue a warrant. The original order in this case appears to have been a traditional search warrant issued under Federal Rule of Criminal Procedure 41. *See* Order at \*1. Such a warrant authorizes law enforcement to search or seize a particular person or property. Fed. R. Crim. P. 41(e). It does not, however, entitle the government to, in seizing property, obtain it in a particular form. In other words, a traditional search warrant allows the government to seize property *as is*, and that authority may not be enlarged through an All Writs Act order compelling a third party to take possession of the property and transform it. For example, if the government had a valid warrant to seize a journal written in a rare foreign language, the All Writs Act could not be used to compel a specialist to translate the journal into English. That authority might make

the information seized more useful, but it is qualitatively different than the underlying authority conferred by the search warrant, and therefore not an appropriate use of the All Writs Act.<sup>1</sup>

In *New York Telephone*, the Supreme Court held that the underlying order requiring installation of a pen register was properly authorized as a “seizure” within the meaning of Rule 41, in the light of Congressional intent to allow the use of pen registers. *See* 434 U.S. at 169–70. Thus, the authority to compel the assistance of the telephone company was implicit in, and necessary to implement, the very seizure authorized by the Rule. *See id.* at 172.

But this case is different. The government’s warrant presumably authorized it to seize an individual’s private mobile device containing personal information, at least some of which has been scrambled using encryption features designed by Apple and turned on, by default, in its “iOS” mobile operating system. Now that the government has seized the device, the warrant’s authority has been exhausted. That the information on the device may still be locked or scrambled does not entitle the government to rely on the warrant authority as a basis for an order under the All Writs Act to compel a third party to transform or provide more useful access to the information seized.<sup>2</sup>

---

<sup>1</sup> In *ITT Community Development Corp. v. Barton*, 569 F.2d 1351 (5th Cir. 1978), the court held that the All Writs Act could not be used to issue a pretrial garnishment order based solely on the district court’s subject matter jurisdiction over a diversity action, because even though doing so would ensure sufficient funds to enforce any eventual judgment, it was not necessary to the court’s jurisdiction to bring the matter to judgment. *See id.* at 1360 (noting “(t)he fact that a party may be better able to effectuate its rights or duties if a writ is issued never has been, and under the language of the statute cannot be, a sufficient basis for issuance of the writ” (quoting *New York Tel. Co.*, 434 U.S. at 189 (Stevens, J., dissenting))). The AWA may be used, of course, to issue remedial orders to effectuate properly authorized judgments or jurisdiction. *See, e.g., Ass’n for Retarded Citizens of Conn., Inc. v. Thorne*, 30 F.3d 367, 370 (2d Cir. 1994) (“Where the district court exercises its jurisdiction to rule on the merits of a litigation, it determines that the law requires a certain outcome and is empowered to issue remedial orders to effectuate that outcome.”).

<sup>2</sup> It remains unclear whether there are other ways for the government to get the information it seeks, including through backup copies of the data stored on Apple’s servers.

**B. The All Writs Act does not confer authority that Congress has consciously withheld.**

As this Court has noted, the All Writs Act cannot be used to substitute for “authority that Congress chose not to confer.” Order at \*2. This is especially true where, as here, the order would impose unprecedented obligations on the third-party recipient of the order and would violate that party’s constitutional rights. *See infra* Part II. In this case, Congress has quite consciously refused to authorize law enforcement to force manufacturers of mobile devices to unlock, and decrypt the data on, those devices. While the government has long had the authority to seize and search documents and tangible objects with a warrant, Congress has never granted law enforcement the authority to force third parties to unlock others’ secure devices or aid in the decryption of data stored on them. And, as demonstrated during recent legislative debates, Congress has made it clear that the decision not to grant that authority was a conscious one.

The last few years have seen robust legislative debates about whether technology companies such as Apple should be required to build “backdoors” into the encryption features now commonly included in computers, mobile devices, and communications software. These “backdoors” would enable law enforcement to access data that might otherwise, in some circumstances, be inaccessible. The debate has included law enforcement, federal agencies, technology experts within the government, and the White House, but has not resulted in congressional action mandating such access.<sup>3</sup> In fact, on the basis of security concerns related to

---

<sup>3</sup> *See* Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, Wash. Post (Apr. 10, 2015), [https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff\\_story.html](https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html); Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S. Over Data Access*, N.Y. Times (Sept. 7, 2015), <http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html>.



enabling such access, the Obama administration reportedly shelved its effort to seek legislation mandating the creation of technological “backdoors” in the encryption used by companies like Apple.<sup>4</sup> Congress has thus far refused, in other words, to give law enforcement what it has asked for: the ability to override the wishes of companies *unwilling* to actively bypass the security built into their products—whether they have the technical capability to do so or not.

In a closely related context, Congress has even more explicitly withheld authority similar to what the government seeks here. The Communications Assistance for Law Enforcement Act (“CALEA”), passed in 1994, requires “telecommunications carriers” to ensure their equipment, facilities, and services are capable of intercepting individuals’ communications in real time. Significantly, when Congress enacted CALEA, it exempted “information services,” which includes certain services that Apple provides, from that requirement. *See* 47 U.S.C. §§ 1002(b)(2), 1001(6)(B)(iii); *see* Order at \*5. In other words, CALEA exempts companies like Apple from the requirement that they build interception features into their communications services and products.

In recent sessions of Congress, the Federal Bureau of Investigation (“FBI”) has vigorously sought to expand CALEA’s reach to cover companies like Apple,<sup>5</sup> in large part because of the widespread migration by consumers from easy-to-intercept telephone calls and text messages to Internet-based communications services that use encryption by default, such as

---

<sup>4</sup> Nicole Perlroth & David E. Sanger, *Obama Won’t Seek Access to Encrypted User Data*, N.Y. Times (Oct. 10, 2015), <http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html>.

<sup>5</sup> *See* Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. Times (Sept. 27, 2010), <http://www.nytimes.com/2010/09/27/us/27wiretap.html>; Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. Times (May 7, 2013), <http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html>.

Apple’s iMessage and Facebook’s WhatsApp services.<sup>6</sup> But the FBI’s proposals have met stiff resistance from Congress, technology experts, and a number of former national security officials. See Andrea Peterson, *Congressman with Computer Science Degree: Encryption Back-doors Are “Technologically Stupid,”* Wash. Post (Apr. 30, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/04/30/congressman-with-computer-science-degree-encryption-back-doors-are-technologically-stupid/> (quoting both Republican and Democratic members of the Information Technology Subcommittee of the House Oversight Committee, several of whom have computer science degrees, criticizing the FBI’s requests for expanded surveillance authorities); Mike McConnell, Michael Chertoff & William Lynn, *Opinion, Why the Fear Over Ubiquitous Data Encryption Is Overblown*, Wash. Post (July 28, 2015), [https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4\\_story.html](https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html) (an op-ed by several former national security officials arguing that “the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level” and that “[i]f law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.”).

In short, Congress has had ample opportunity, in multiple contexts, to compel companies such as Apple to build surveillance mechanisms into their products and services to facilitate government access, but it has declined to do so. It has refused, during the debate of the last

---

<sup>6</sup> See Ellen Nakashima, *WhatsApp, Most Popular Instant-Messaging Platform, to Encrypt Data for Millions*, Wash. Post (Nov. 18, 2014), [https://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6\\_story.html](https://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html).

several months, to compel companies like Apple to build backdoors into the encryption used to protect data *stored* on mobile devices. And, both when it passed CALEA in 1994, and in the recent debate regarding the expansion of CALEA sought by the FBI, it has refused to require companies like Apple to build surveillance mechanisms necessary to enable the government to *intercept* otherwise encrypted digital communications.

This case, thus, stands in stark contrast to *New York Telephone*, in which the Supreme Court observed that Congress had intended to allow the use of pen registers. The Supreme Court, in part on that basis, decided that a telephone company could be compelled to assist with the installation of a pen register. *See New York Tel. Co.*, 434 U.S. at 176 (“Congress clearly intended to permit the use of pen registers by federal law enforcement officials.”); *id.* at 170 (noting that where Congress had already permitted “the recording of conversations by means of electronic surveillance” it would be “anomalous” to find that Congress intended to prohibit “the far lesser intrusion accomplished by pen registers.”); *see also In re Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 579 (D. Md. 2011) (“[T]he All Writs Act enables the Court to, in the absence of other enabling authority, issue supplemental orders to effectuate valid orders or warrants issued under existing law, but only to the extent any supplemental order issued does not constitute an additional invasion of privacy. Notably, and critically different than this matter, *the Supreme Court acknowledged and deferred to congressional approval of a pen register as a permissible law enforcement tool.*” (emphasis added)).<sup>7</sup>

---

<sup>7</sup> *See also Application of the U.S.*, 427 F.2d 639, 644 (9th Cir. 1970), *superseded by statute* (holding that because there was no statutory authorization, a federal district court could not compel a telephone company to provide technical cooperation in intercepting a wire communication) (later superseded by amendments to Title III, 18 U.S.C. §§ 2511, 2518 & 2520, providing express authority for assistance in certain circumstances).

For these reasons, the All Writs Act may not be used to compel Apple to unlock or decrypt its customers' devices. That Apple may have created for its own use tools that can extract at least some private data from some devices is irrelevant to whether *Congress* intended to grant law enforcement agencies the authority to demand the creation or use of such tools and capabilities by third parties. Congressional intent is the critical factor in determining whether the All Writs Act can be used to issue the order here. Because Congress consciously withheld that authority, the All Writs Act cannot be used to confer it.

**II. It would be unconstitutional to conscript Apple into governmental service to assist in gaining access to information that Apple does not possess or control.**

Even if the All Writs Act could be stretched to permit it, the compelled assistance the government seeks from Apple is unconstitutional. Third parties cannot be commissioned to work for law enforcement except in narrow contexts, which do not include simply being the manufacturer of a device containing stored personal information which the third party does not possess or control. The government seeks to compel a third party not accused of wrongdoing to create information—derived from information that the party does not possess or control—and to provide that information to law enforcement. Compelling a device's manufacturer to unlock or decrypt the private data stored on the device is akin to compelling a lock manufacturer to break into the houses of its customers for the government. This type of assistance to law enforcement is qualitatively different from cases where *the very information* the government seeks is within the third party's possession or control.

The government's request in this case implicates fundamental liberty and property interests, and thus raises novel and grave constitutional questions regarding the limits on the

assistance the government can compel from private actors.<sup>8</sup> At the very least, those questions trigger this Court’s obligation, under the doctrine of constitutional avoidance, to interpret the All Writs Act not to permit the sort of order the government seeks here. *See Clark v. Martinez*, 543 U.S. 371, 380–81 (2005) (“[W]hen deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude of constitutional problems, the other should prevail—whether or not those constitutional problems pertain to the particular litigant before the Court.”).

It is already established that governmental conscription of third parties’ assistance is of constitutional import. As this Court and others have recognized, an order compelling third-party conduct pursuant to the All Writs Act necessarily implicates the third party’s due process rights under the Fifth Amendment. *See Order at \*10; Application of U. S. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder & Terminating Trap (Bell Telephone)*, 610 F.2d 1148, 1156 (3d Cir. 1979) (“We have no difficulty finding a deprivation of a property interest here. The tracing orders denied appellants the free use of their equipment and of the services of their employees, interests to which they are entitled as basic property and contract rights.”).

Because an order under the All Writs Act burdens fundamental interests in property and liberty, courts have held that a third party recipient of such an order is entitled to a hearing at which to contest it.<sup>9</sup> While that hearing fulfills the procedural protections guaranteed by the Fifth

---

<sup>8</sup> This Court need not decide what precise connection a third party must have to the underlying information the government seeks before it may be compelled to assist. It is enough in this case that Apple does not possess the data stored on the device, and that the information sought by the government here is not traveling through any medium that Apple controls.

<sup>9</sup> *See, e.g., Bell Telephone*, 610 F.2d at 1157 (“We conclude that due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide tracing assistance.”); *Application of U.S. for an Order Authorizing an In-Progress Trace of Wire*

Amendment, courts have also recognized a *substantive* limit on the authority to compel assistance from third parties: the assistance may not be unreasonably burdensome. *See New York Tel. Co.*, 434 U.S. at 172 (“[T]he power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed.”); *see also Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc’ns over Tel. Facilities (Mountain Bell)*, 616 F.2d 1122, 1132–33 (9th Cir. 1980) (affirming a district court’s order compelling Mountain Bell to trace telephone calls by using electronic facilities within the company’s exclusive control, on the ground that “the obligations imposed . . . were reasonable ones.” (citing *New York Tel. Co.*, 434 U.S. at 172)).

Indeed, Apple’s Fifth Amendment interests here are particularly acute. Among those interests is the maintenance of business goodwill, *i.e.*, the “expectancy of continued patronage,” which constitutes a protected property interest. *Newark Morning Ledger Co. v. United States*, 507 U.S. 546, 555 (1993) (internal quotation marks omitted); *see Soranno’s Gasco, Inc. v. Morgan*, 874 F.2d 1310, 1316 (9th Cir. 1989) (“The goodwill of one’s business is a property interest entitled to protection; the owner cannot be deprived of it without due process.”); *Glosband v. Watts Detective Agency, Inc.*, 21 B.R. 963, 975 (D. Mass. 1981) (“Goodwill is a right of property which the courts will guard as carefully as it would visible, tangible property.” (internal quotation marks omitted)). Apple expressly distinguishes itself on the basis of its commitment and ability to protect users’ privacy and security. *See, e.g.*, Matthew Panzarino,

---

*Commc’ns over Tel. Facilities*, 616 F.2d 1122, 1132–33 (9th Cir. 1980) (declining to rule on a due process challenge to compelled assistance by a telephone company because it was not raised below but nonetheless ordering that the third party be given “reasonable notice and an opportunity to be heard” given the “important nature of the interests at stake”); *In re XXX, Inc.*, No. 14 Mag. 2258, 2014 WL 5510865, at \*2 (S.D.N.Y. Oct. 31, 2014) (“Courts have held that due process requires that a third party subject to an order under the All Writs Act be afforded a hearing on the issue of burdensomeness prior to compelling it to provide assistance to the Government.”).

*Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy*, TechCrunch (June 2, 2015), <http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy>. In doing so, it is participating in the new market that U.S. technology companies are now actively competing in, based on the privacy and security features built into their products. See Electronic Frontier Foundation, *Who Has Your Back*, <https://www.eff.org/who-has-your-back-government-data-requests-2015> (last visited Oct. 19, 2015); Letter from Yahoo! Inc. to U.S. Marshals Service, at 9 (Sept. 15 2009), [http://www.wired.com/images\\_blogs/threatlevel/2009/12/yahoo-price-list-letter.pdf](http://www.wired.com/images_blogs/threatlevel/2009/12/yahoo-price-list-letter.pdf) (noting that the release of information about Yahoo! turning over users' data to law enforcement is "reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies."). The assistance the government seeks here would undermine Apple's commitment and ability to protect its users' privacy, exacerbating the property deprivation.

While there is little precedent interpreting the substantive limits on the government's authority to compel assistance in its investigations, *amici* contend that the Fifth Amendment forbids the government from compelling the assistance it seeks here: the assistance of an unwilling third party not accused of wrongdoing to obtain information it does not possess or control. Aside from the government's recent efforts to compel the unlocking of mobile devices, *amici* are not aware of any case in our country's history allowing the government to compel such assistance. That sort of "assistance" is fundamentally inconsistent with the interests protected by the Fifth Amendment, which generally guarantees freedom from governmental interference

absent evidence of wrongdoing or possession or control of information to which the government is entitled.<sup>10</sup>

Although prior cases compelling assistance from third parties have not addressed the substantive due-process question raised here, they are all consistent with the view *amici* advance. In those cases, compelled assistance was deemed permissible where it involved third parties that possessed the information the government wanted or that controlled the medium through which the information traveled. In fact, in *New York Telephone*, the Supreme Court specifically considered whether the telephone company in the case “was a third party *so far removed from the underlying controversy* that its assistance could not be permissibly compelled.” 434 U.S. at 174 (emphasis added). This language suggests a limit on the *types* of innocent third parties the government can coerce into assisting it, regardless of the material burden imposed on that party. In *New York Telephone*, for example, it was important to the Supreme Court’s analysis that the third party’s facilities “were being employed to facilitate a criminal enterprise on a continuing basis.” *Id.* at 174–75. But in this case, Apple is not connected to the underlying investigation—it simply manufactured and sold the device that stores the data the government wants as part of an investigation unrelated to Apple. Another factor *New York Telephone* emphasized was the telephone company’s role as a “highly regulated public utility *with a duty to serve the*

---

<sup>10</sup> *Amici* are aware of one opinion and two orders that have been made public compelling the unlocking of a mobile device. In the published opinion addressing this issue, the court noted that its decision was rendered prior to satisfying the procedural due process requirements implicated by such an order. *See In re XXX, Inc.*, No. 14 Mag. 2258, 2014 WL 5510865, at \*2–\*3 (S.D.N.Y. Oct. 31, 2014). And, as this Court noted, *In re XXX, Inc.* failed to consider the burden of compliance beyond “the physical demands and immediate monetary costs.” Order at \*9. The two other orders compelling the unlocking of mobile devices did not address the constitutional concerns raised by such an order. In both cases, the courts declined to compel Apple to attempt to decrypt or enable access to encrypted data. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, CR 14-90812, \*2 (N.D. Cal. Nov. 3, 2014); *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, CR 14-90470, \*1 (N.D. Cal. June 6, 2014).



*public . . .*” *Id.* at 174 (emphasis added). But in this case, Apple is a private company competing on the very basis of the privacy and security it can offer its customers. Moreover, it is doing so in an environment where the use of encryption to protect data stored on mobile devices has been actively encouraged by legislators and law enforcement officials. *See supra* Part I.B.

Thus, two critical factors distinguish this case from *New York Telephone*: in *New York Telephone*, (1) the recipient of the All Writs Act order possessed or had effective control over the very information the government sought, and (2) the telephone company had no business interest that would be harmed. *See* 434 U.S. at 174–75 (“[I]t can hardly be contended that the Company . . . had a substantial interest in not providing assistance.”). The same factors are present in essentially all relevant cases compelling assistance. For example, the Ninth Circuit held that a district court had the power under the All Writs Act to order a telephone company to “perform an *in-progress* trace of telephone calls by means of electronic *facilities within its exclusive control.*” *Mountain Bell*, 616 F.2d at 1123 (emphases added). In so holding, the court emphasized the narrowness of its ruling, stating “our decision today should not be read to authorize the wholesale imposition upon private, third parties of duties pursuant to search warrants.” *Id.* at 1132; *see also United States v. Doe*, 537 F. Supp. 838, 840 (E.D.N.Y. 1982) (granting an order, pursuant to the All Writs Act, to compel a telephone company to supply a subscriber’s toll records within its possession); *Bell Telephone*, 610 F.2d at 1155 (finding that the district court could, pursuant to the All Writs Act, order a telephone company to assist law enforcement agents in the tracing of telephone calls); *United States v. Hall*, 583 F. Supp. 717 (E.D. Va. 1984) (holding the government was entitled to a court order, pursuant to the All Writs Act, compelling a credit card issuer to duplicate and provide credit card records the company already maintained); *In re Application of U.S. for an Order Directing X to Provide Access to*

*Videotapes*, No. 03-89, 2003 WL 22053105, at \*3 (D. Md. Aug. 22, 2003) (finding appropriate an order under the All Writs Act that directed an apartment complex “merely to provide access” to the government to videotapes the apartment complex possessed); *In re Application of U.S. for an Order Directing a Provider of Comm’n Servs. to Provide Technical Assistance to Agents of the U.S. Drug Enforcement Admin.*, No. 15-1242 M, 2015 WL 5233551, at \*5 (D.P.R. Aug. 27, 2015) (issuing an order under the All Writs Act directing an electronic communication services provider to facilitate the *interception* of electronic communications to and from a mobile phone where the mobile phone customer had consented).

In this case, Apple does not possess the device the government has seized or the private data the government seeks. The government is neither requiring Apple to intercept information that passes through its control, as in the telephone company cases, nor compelling Apple to obtain records that the company maintains.

Furthermore, unlike in previous cases, the order here would fundamentally alter the relationship between Apple and its customers, against its will. The Ninth Circuit considered the impact on a third party’s business model when assessing the limits of compelled assistance to law enforcement, even though it did not explicitly consider constitutional limits. In *The Company v. United States*, 349 F.3d 1132 (9th Cir. 2003), the court concluded that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2518, provides for wiretap orders requiring third parties to assist law enforcement where they “can arrange access to facilities or technical assistance necessary to intercept communications.” *Id.* at 1142.

Nonetheless, the court concluded that Title III did not authorize an order allowing the FBI to force a company to wiretap conversations taking place in a car by using the microphone installed in the car as part of the company’s on-board communications system. *Id.* at 1146. In finding such

assistance impermissible, the court noted that “[t]he 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, and, as we read title III, Congress did not intend that it would.” *Id.* at 1145. Because the result of compelling assistance to the FBI would have been such that “the Company could no longer supply any of the various services it had promised its customer, including assurance of response in an emergency,” the court held that Congress could not have intended for such assistance to be required by Title III. *Id.* at 1146.<sup>11</sup>

The same logic applies here. The governmental compulsion in this case would fundamentally alter Apple’s ability to market a secure device to its customers.<sup>12</sup>

For these reasons, the order the government seeks here violates the Fifth Amendment. It would constitute a dramatic and unwarranted expansion of the government’s investigative authority, by permitting it to conscript into government service those who have done nothing wrong and who do not possess or control information to which the government is entitled.

---

<sup>11</sup> The Ninth Circuit noted that the district court in the case had found that such an order would violate both the Takings Clause and the Due Process Clause, but the company withdrew its constitutional challenges on appeal. *See The Company*, 349 F.3d at 1135 n.6.

<sup>12</sup> As *amici* understand it, the two most recent versions of Apple’s mobile operating system encrypt data in a more secure way than previous versions, such that Apple is unable to extract the data from users’ devices, even if the company wishes to do so. Only a small and diminishing percentage of devices in use run a version of the operating system that Apple has the capability to unlock and extract data from. Although Apple previously maintained the ability to unlock certain devices for law enforcement agencies, it is free to choose to no longer maintain that technical ability or to discontinue offering it to law enforcement. In other words, just because a device manufacturer *could* unlock and decrypt the data on a device, and has done so in the past voluntarily, does not create an ongoing obligation for the company to continue to offer that service to the government in the future.

## CONCLUSION

For these reasons, the Court should deny the government's request. *Amici* respectfully request the opportunity to participate in any oral argument held.

Date: October 19, 2015

Respectfully Submitted,

/s/ Esha Bhandari

Arthur Eisenberg  
Mariko Hirose  
New York Civil Liberties Union  
125 Broad Street, 19th Floor  
New York, NY 10004  
Tel: 212-607-3300  
aeisenberg@nyclu.org

Esha Bhandari\*\*  
Alex Abdo  
American Civil Liberties Union  
Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
Tel: 212-549-2500  
ebhandari@aclu.org

Jennifer Stisa Granick (CA Bar #168423)  
Director of Civil Liberties\*  
Riana Pfefferkorn (CA Bar #266817)  
Cryptography Policy Fellow\*  
Stanford Law School  
Center for Internet and Society  
559 Nathan Abbott Way  
Stanford, CA 94305  
Tel: 650-736-8675  
jennifer@law.stanford.edu  
\* For affiliation purposes only

Andrew Crocker  
Nathan D. Cardozo  
Electronic Frontier  
Foundation  
815 Eddy Street  
San Francisco, CA 94109  
Tel: 415-436-9333  
andrew@eff.org

\*\*Counsel for *amicus curiae* the American Civil Liberties Union wish to thank Eliza Sweren-Becker and Christopher Soghoian for their assistance in preparing this brief.