

**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 device¹ but, as requested by the Court, Apple will limit its response to the topics of feasibility and burden.²

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

¹ 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.

² 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 (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.³ 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

³ 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