SDD/ZA:SK/LHE/AK
F. #2014R00236

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

– –X

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

Docket Nos.: 15-MC-1902 (JO), 14-CR-387 (MKB)

– –X

THE GOVERNMENT'S MEMORANDUM OF LAW IN SUPPORT OF ITS APPLICATION FOR AN ORDER COMPELLING APPLE INC. TO ASSIST LAW ENFORCEMENT AGENTS IN THE EXECUTION OF A SEARCH WARRANT

ROBERT L. CAPERS
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

Saritha Komatireddy
Lauren Howard Elbert
Ameet Kabrawala
Assistant U.S. Attorneys
Eastern District of New York

Nathan Judish
Jared Hosid
Senior Counsel
Computer Crime and
Intellectual Property Section
Department of Justice
(Of Counsel)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES

RULES

PRELIMINARY STATEMENT

This is a routine application asking the Court to order a third party to assist in the execution of a search warrant. The Department of Justice has made the same application, for the same assistance, from the same company, dozens of times before. Federal courts around the nation have granted these applications. The company has complied every time. Until now.

In mid-2014, law enforcement agents arrested Jun Feng on charges related to his participation in a methamphetamine distribution conspiracy. Agents conducted a search of Feng's home, pursuant to a warrant, and seized an Apple iPhone 5s running iOS 7. The government subsequently obtained a warrant to search the phone. The government is unable to access the data on the phone, however, because the phone is locked with a passcode. The government cannot bypass the lock screen without risking data destruction. Apple can. Apple has extracted data from iPhones like this one pursuant to All Writs Act orders numerous times, including as a result of orders issued in the Eastern District of New York. Apple has confirmed that it can do so again, in this case, with this phone, and that doing so would pose no significant burden to the company.

On October 8, 2015, the government applied to United States Magistrate Judge James Orenstein, serving as duty magistrate, for an order under the All Writs Act, 28 U.S.C. § 1651, requiring Apple to provide reasonable technical assistance to enable access to the data on Feng's phone. On February 29, 2016, the magistrate judge denied the government's application. See ECF No. 29. Because this Court maintains supervisory authority over the underlying matter, the government respectfully resubmits its application to this Court and moves this Court to grant the government's application for an All Writs Act order.

In light of the debate that has recently come to surround this issue, it is worth briefly noting what this case is not about. Apple is not being asked to do anything it does not currently have the capability to do. All of Apple's pre-iOS 8 operating systems allowed for extracting data from a passcode-locked device. Apple has used that capability dozens of times, in response to lawful court orders like the one sought here, with no claim that doing so put customer data or privacy in harm's way. Apple may perform the passcode-bypass in its own lab, using its own technicians, just as it always has, without revealing to the government how it did so. Therefore, granting the application will not affect the technological security of any Apple iPhone nor hand the government a "master key."

This case in no way upends the balance between privacy and security. The Constitution has already struck the relevant balance: it protects the people's privacy "in their persons, houses, papers, and effects," but permits reasonable searches including ones where the government has a warrant. Here, the government has a warrant. And a longstanding federal statute provides this Court with the authority to require Apple to assist with that warrant. Requiring that assistance does not "intensif[y] the nature of the incursion on [] privacy" or disturb the Constitution's carefully considered balance. See United States v. Zaragoza, No. 12-CR-20119, ECF No. 65 at 2-3 (S.D. Fl. July 12, 2012) (commenting on an All Writs Act order requiring Apple to perform a passcode-bypass). It simply enables this Court to ensure that its warrant has meaning.

STATEMENT OF FACTS

The Apple iPhone 5s running iOS 7 that is the subject of the government's application was seized pursuant to a search warrant from the residence of Jun Feng, a defendant in a criminal case before this Court. Feng was indicted on three counts related to the possession and distribution of methamphetamine. See United States v. Jun Feng, No. 14-CR-387, ECF No. 98 (E.D.N.Y. July 15, 2015). On October 29, 2015, Feng pleaded guilty to conspiring with others to distribute and possess with intent to distribute methamphetamine. During his plea, Feng stated that he sold "ice" (crystal methamphetamine) in Queens, New York, "with other people." Feng, ECF No. 119 at 21. The government's investigation into the methamphetamine conspiracy is ongoing.

On July 6, 2015, the Honorable Viktor V. Pohorelsky, United States Magistrate Judge for the Eastern District of New York, issued a search warrant for the iPhone seized from Feng's residence. See In re Cellular Telephone Devices Seized et al., No. 15-M-610 (E.D.N.Y. July 6, 2015). However, despite the search warrant, the government has been unable to access the contents of Feng's phone because it is locked by a passcode. Moreover, the government has been unable to attempt to determine the passcode because Apple has written its operating systems with a user-enabled "auto-erase" feature that would, if enabled, render the data on the device permanently inaccessible after multiple failed passcode attempts. When an Apple iPhone is locked, it is not apparent whether or not that auto-erase feature is enabled; therefore, trying repeated passcodes risks permanently denying all access to the contents of the phone. As a result, the government cannot access the contents of the phone and execute the warrant without Apple's assistance.

The government also does not have an alternative means of obtaining information from the phone. The settings on Feng's phone do not permit access to data without entering the correct passcode. The contents of Feng's phone were not backed up or otherwise copied onto Apple's iCloud cloud storage service. The phone also has a remote wipe request pending, such that if the phone were powered on and connected to a network, the pending request would direct the erasure of the encryption keys necessary to decrypt the data on the phone, making it permanently inaccessible.[1]

Apple is the manufacturer of the iPhone Model 5s and the creator and owner of the iOS operating system. Apple maintains strict control over what operating system software may run on iPhones, designing iPhones to only run operating system software designed and signed by Apple, i.e., iOS. The iOS operating system on Feng's phone contains a passcode feature that locks the phone and prevents access to its contents. For versions of the operating system that pre-date iOS 8 — including version iOS 7, which is installed on Feng's phone — Apple has the technological capability to bypass the passcode feature and access the contents of the phone that were unencrypted. ECF No. 11 at 2-3.

The passcode-bypass process involves sending the device to Apple's headquarters in Cupertino, California, where Apple technicians, in an Apple lab, bypass the passcode and extract the phone's data. Apple's method for performing the bypass is not

[1] Apple's remote wipe feature is one aspect of Apple's ongoing provision of service to iPhone owners, even when the service can interfere with execution of a warrant. Apple has confirmed that someone activated the remote wipe feature on Feng's phone. Apple has further confirmed that it has not taken any action to disable the feature. ECF No. 19 ("Hr'g Tr.") at 32. Apple also suggests that the feature will not function at this time. Id. at 32-33. These representations appear to conflict, and Apple has not further explained why the requested remote wipe cannot take effect.

shared or revealed to the government during this process. Apple technicians then return the device and a copy of the extracted data to law enforcement agents so that the agents may conduct their search.

Given this capability, Apple has developed guidance for law enforcement agents for obtaining lawful court orders to request such a bypass. Apple states in its Legal Process Guidelines, which Apple makes publicly available online and provides to law enforcement to this day, that "for iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices." See "Extracting Data from Passcode Locked iOS Devices," Apple Legal Process Guidelines § III(I) (last accessed Mar. 2016), http://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf, attached hereto as Exhibit D. Apple's guidelines also express a preference for specific language to be included in the order directed to it and how such an order should be served. Id. Apple states in its guidelines: "Once law enforcement has obtained a search warrant containing this language, it may be served on Apple by email . . . . After the data extraction process has been completed, a copy of the user generated content on the device will be provided." Id.

On October 7, 2015, prior to its initial application for an order in this matter, the government contacted Apple via email through its law enforcement liaison, noted that it may seek to obtain an order directing Apple to assist in the passcode-bypass of an iPhone 5s, and inquired how long it would take for Apple to extract data pursuant to such an order. Shortly thereafter, an Apple data extraction specialist responded and informed the government, in pertinent part, that "for iOS devices running pre iOS 8, upon receipt of a

valid search warrant pursuant to the instructions laid out in [the legal process guidelines], Apple can extract certain categories of active data from passcode locked iOS devices. Before submitting your search warrant, please validate that the targeted device is running pre iOS 8."

The government then responded and informed Apple that Feng's phone was running an operating system that was "pre iOS 8." Apple responded, "Upon receipt of a valid search warrant pursuant to the instructions laid out in [the legal process guidelines], we can schedule the extraction date within a 1-2 week time frame."

At no time during these communications did Apple object to the propriety of the government's proposed order directing Apple's assistance or indicate that compliance would impose any burden. To the contrary, on more than one occasion, Apple provided the government with specific requests for the language it preferred in court orders and instructions for effectuating such an order. See Ex. D, § III(I).

The following day, on October 8, 2015, the government applied to United States Magistrate Judge Orenstein, serving as duty magistrate, for an order pursuant to the All Writs Act, directing Apple to provide "reasonable technical assistance" to enable law enforcement agents to access the data on Feng's phone. With its application, the government submitted a proposed order that incorporated the language that Apple requested in its Legal Process Guidelines.

On October 9, 2015, Judge Orenstein issued a memorandum and opinion deferring the government's application and ordering briefing on the technical feasibility and burden to Apple of complying with the proposed order. ECF No. 2. On October 19, 2015, Apple filed a brief in which, for the first time ever, it objected to the government's use of the

All Writs Act. ECF No. 11. On October 26, 2015, the magistrate judge heard oral argument from the parties.

Apple represents to its customers that when it receives a court order, "If there is any question about the legitimacy or scope of the court order, we challenge it," noting that it complies "[o]nly when we are satisfied that the court order is valid and appropriate." See Report on Government Information Requests at 2, Apple Inc. (Nov. 5, 2013). In its briefing and oral argument in this case, Apple conceded that it never previously objected to any of the numerous All Writs Act orders it has received. See ECF No. 16 at 3 (Apple "has never taken any position on whether All Writs Act orders in aid of search warrants are legally appropriate" and "Apple did not challenge the underlying authority of the court to issue the orders"). Apple acknowledged that the routine issuance of All Writs Act orders indicated that "the weight of the authority" supported their issuance and "it seemed that this had been somewhat settled views and settled authority from multiple judges." Hr'g Tr. at 55-56. Apple further stated that "it has, in prior instances, complied with data extraction demands" contained in search warrants and All Writs Act orders. ECF No. 16 at 3.

Apple made clear that its objection in this case arose because the magistrate judge required Apple's intervention prior to the order's issuance. ECF No. 16 at 3-4; Hr'g Tr. at 55 (counsel for Apple stating that no court had previously "invited Apple to submit its views"). In other words, Apple indicated that, given the public attention directed to the case by the magistrate judge, Apple's public relations concerns prompted it to object. See Hr'g Tr. at 58. However, Apple also made it clear that, if the court issued an All Writs Act order, it would comply. See Hr'g Tr. at 10 (counsel for Apple stating that "Apple would comply with an order of this court"); see ECF No. 16 at 11 ("Of course, Apple takes its obligations as

a corporate citizen very seriously, which is why it routinely provides assistance to law enforcement where there is a proper legal basis for it to do so.").

During the briefing, Apple represented that it could perform the passcode-bypass in as little as one day, and at oral argument, its counsel specified that the process only takes "several hours." Hr'g Tr. at 25.

A few days after oral argument, on October 29, 2015, Feng pleaded guilty to conspiring to distribute and possess with intent to distribute methamphetamine. In light of that development, Judge Orenstein ordered the government to explain why its application for Apple's assistance was not rendered moot by the guilty plea. The government filed a letter stating that its investigation into the narcotics conspiracy is ongoing, that Feng's sentencing is still pending, and that the search warrant for the phone authorized seizing evidence related to Feng and others, including his "customers" and "sources." ECF No. 25 at 1. The magistrate judge issued no further orders and did not rule on the government's application at that time.

On February 12, 2016, Apple filed a letter agreeing that the matter is not moot, stating that it has received additional similar requests, and requesting a ruling from the magistrate judge. On February 16, 2016, Judge Orenstein ordered Apple to provide additional information, under seal, about the other requests it had received and whether Apple had objected to those requests; the magistrate judge ordered the government to respond thereafter with any proposed redactions. On February 17, 2016, Apple filed a letter under seal with the additional information, listing twelve All Writs Act orders it had received over the past five months ("Apple's List"), in addition to a well-publicized order in San Bernardino, California, and claiming that it had objected to most of the All Writs Act orders

listed therein. ECF No. 27. On February 22, 2016, the government filed a public response stating that it was not requesting any redactions, emphasizing that Apple's List showed that numerous judges around the country had found it appropriate to use the All Writs Act to direct Apple to assist law enforcement in accessing Apple devices, and pointing out that Apple did not challenge any of those orders in court, as they had suggested, but had instead deferred complying with them. ECF No. 28.

Meanwhile, in the Central District of California, on February 16, 2016, the government obtained an All Writs Act order requiring Apple to assist law enforcement in accessing the phone of one of the shooters involved in the mass murders in San Bernardino, California. See In re the Search of an Apple iPhone, No. 15-M-0451 (C.D. Cal. Feb. 16, 2016). Apple is litigating that matter. The iPhone at issue in the San Bernardino case involves a different model of phone with a different version of iOS.

As noted above, Apple has an established track record of assisting law enforcement agents by extracting data from passcode-locked iPhones pursuant to court orders issued under the All Writs Act. The government has confirmed that Apple has done so in numerous federal criminal cases around the nation. In the course of handling these requests, Apple has, on multiple occasions, extracted data from a passcode-locked device and provided the government with the specific language it demands in the form of a court order to do so. To cite just a few examples:

- In 2008, approximately one year after the release of the first iPhone, the government obtained a search warrant for an iPhone in a child exploitation case in the Northern District of New York, in which the defendants had drugged and sexually abused several minor children. The government consulted with Apple regarding the passcode lock on the phone, and an Apple representative advised the government in an email: "Per your request, I am sending you some proposed language that Apple requires in the form of a

court order, which could be entered in conjunction with a search warrant, in order to bypass a user's iPhone passcode." The government obtained an All Writs Act order with Apple's requested language. Law enforcement agents then flew to Apple's headquarters in California with the iPhone and Apple bypassed the phone's passcode and extracted data from it immediately, in the agents' presence. Both defendants pleaded guilty to child exploitation charges and were sentenced to life imprisonment. See United States v. Jansen, No. 08-CR-753 (N.D.N.Y. 2010).

- In a narcotics case in the Middle District of Florida, in which the defendant conspired to possess methylone with intent to distribute it, law enforcement agents obtained an All Writs Act order directing Apple to assist in extracting data from a passcode-locked iPhone. After approximately five months, Apple extracted the data from the iPhone and provided that data to law enforcement agents on a flash drive. The case went to trial and the parties entered into a stipulation regarding the data extraction so that Apple would not be required to testify. The defendant was convicted at trial and sentenced to five years' imprisonment. See United States v. Bellot, No. 14-CR-48 (M.D. Fla. 2015).

- In a case in the Western District of Washington, in which the defendant sexually exploited children and produced child pornography, law enforcement agents obtained an All Writs Act order directing Apple to assist in extracting data from the defendant's passcode-locked iPhone, over the defendant's objection. Apple estimated that it would take approximately four months to extract the data from the phone. After the district court directed Apple to comply within one month or otherwise show cause, so that the data could be available for trial, Apple extracted the data and provided it to law enforcement within ten days. The defendant pleaded guilty and was sentenced to twenty-three years' imprisonment. See United States v. Navarro, No. 13-CR-5525 (W.D. Wa. 2013).

The government is not aware of any instances prior to this case in which Apple objected to such an order; indeed, Apple routinely complied with such orders.

On February 29, 2016, Judge Orenstein determined that, in light of the government's ongoing investigation, the government's application is not moot; however, the magistrate judge denied the application. See ECF No. 29.

The gravamen of Judge Orenstein's opinion was that the All Writs Act relief that the government requests in this case is "unavailable because Congress has considered

legislation that would achieve the same result but has not adopted it." ECF No. 29 at 1. The magistrate judge held that the Court is therefore precluded by the terms of the statute from granting such relief. Id. Despite this conclusion, the magistrate judge proceeded to opine that, were he not so precluded, he would nevertheless deny the government's application for an All Writs Act order because the circumstances of this case do not "justif[y] imposing on Apple the obligation to assist the government's investigation against its will." ECF No. 29 at 1.

For the reasons set forth below, the government respectfully submits that the Court has the authority pursuant to the All Writs Act to issue the proposed order in this case, and that the circumstances of the case warrant such relief. The government further submits that this Court should not adopt Judge Orenstein's legal analysis because that analysis goes far afield of the circumstances of this case and sets forth an unprecedented limitation on federal courts' authority pursuant to the All Writs Act to issue orders in aid of their jurisdiction. Accordingly, the government respectfully requests that the Court grant the application.

ARGUMENT

I. This Court Has Jurisdiction Over the Application for an Order Requiring Apple's Assistance

The All Writs Act provides in relevant part that "all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). The magistrate judge's authority to review All Writs Act applications falls within the authority granted by Section 636(b)(3) of the Federal Magistrates Act. See 28 U.S.C. § 636(b)(3) ("A

magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States."); see also E.D.N.Y. Local Criminal Rule 59.1(c) (applying E.D.N.Y. Local Civil Rule 72.1 in criminal proceedings); E.D.N.Y. Local Civil Rule 72.1(c) (providing that magistrate judges may issue orders necessary to obtain evidence needed for court proceedings).

This Court continues to preside over the criminal case against Jun Feng, the owner of the iPhone at issue, and retains "supervision and control" of matters delegated to magistrate judges in connection with the Feng investigation. In re Application of the U.S. for an Order of Nondisclosure, 41 F. Supp. 3d 1, 4 (D.D.C. 2014) (citing In re Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 289 (4th Cir. 2013)). Therefore, the government may resubmit its application to this Court for de novo review following its denial by the magistrate judge. Id. (review "must be de novo"); see, e.g., In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011) (Garaufis, J.) (considering the government's resubmitted application de novo after its denial by the magistrate judge); In re Application of the U.S. for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (same).[2]

All Writs Act applications for orders requiring third-party assistance are ordinarily submitted and adjudicated ex parte. See, e.g., United States v. New York Telephone Co., 434 U.S. 159, 161-63 (1977); In re Application of U.S. for an Order

[2] The government's application is attached hereto as Exhibit A; the proposed order is attached hereto as Exhibit B; and the underlying search warrant is attached hereto as Exhibit C.

Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities, 616 F.2d 1122, 1123 (9th Cir. 1980) (hereinafter, "Mountain Bell"); In re Application of U.S. for an Order Directing a Provider of Commc'n Servs. to Provide Tech. Assistance to Agents of the DEA, No. 15-M-1242, 2015 WL 5233551, at *1 (D.P.R. Aug. 27, 2015); In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant by Unlocking a Cellphone, No. 14-M-2258, 2014 WL 5510865, at *1 (S.D.N.Y. Oct. 31, 2014) (hereinafter, "In re [XXX]"); In re Application of U.S. for an Order Directing X to Provide Access to Videotapes, No. 03-89, 2003 WL 22053105, at *1 (D. Md. Aug. 22, 2003) (hereinafter, "Access to Videotapes"). Ex parte consideration has been found to be appropriate because "orders providing technical assistance of the kind sought here are often not deemed to be burdensome." In re [XXX], 2014 WL 5510865, at *2 (citing cases).

While third parties retain the right to determine whether to object, the opportunity to object after the issuance of the order has been deemed sufficient to vindicate that right. See In re [XXX], 2014 WL 5510865, at *2 (for All Writs Act orders, due process satisfied by providing for a post-issuance opportunity to object); cf. In re Application of the U.S. for an Order of Nondisclosure, 41 F. Supp. 3d 1, 6 (D.D.C. 2014) (for non-disclosure applications, reversing magistrate judge's order inviting third party to intervene and considering it sufficient that statute provided third party with a post-issuance opportunity to object); Fed. R. Crim. P. 17(c)(2) (for subpoenas, providing recipients with post-issuance opportunity to object). Courts have found ex parte adjudication in the first instance to be the proper procedure even where the third party was expected to object. See In re the Search of an Apple iPhone, No. 15-M-0451 (C.D. Cal. Feb. 16, 2016). However, in light of the fact that Judge Orenstein already compelled Apple to participate here, and in light of Apple's

subsequent participation in briefing and oral argument before the magistrate judge, the government does not object to the Court inviting a submission from Apple, should the Court determine such a submission appropriate.

II. The All Writs Act Authorizes the Order at Issue Here

The All Writs Act provides in relevant part that "all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). The government's application requests that this Court issue an order requiring Apple to provide reasonable technical assistance — specifically, to perform a passcode-bypass — that is necessary and appropriate in aid of the Court's search warrant for Feng's phone.

The All Writs Act permits a court, in its "sound judgment," to issue orders necessary "to achieve the rational ends of law" and "the ends of justice entrusted to it." New York Telephone Co., 434 U.S. at 172-73 (citations and internal quotation marks omitted). Courts must apply the All Writs Act "flexibly in conformity with these principles." Id. at 173; accord United States v. Catoggio, 698 F.3d 64, 67 (2d Cir. 2012) ("[C]ourts have significant flexibility in exercising their authority under the Act." (citation omitted)).

In New York Telephone Co., the Supreme Court held that courts have All Writs Act authority to issue supplemental orders to third parties to facilitate the execution of search warrants. The Court held that:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, . . . and encompasses even those who have not taken any affirmative action to hinder justice.

Id. at 174 (citation omitted).

In particular, the Court upheld an order directing a phone company to assist in executing a pen register search warrant issued under Rule 41 of the Federal Rules of Criminal Procedure. See id. at 171-76. Under New York Telephone Co., the All Writs Act provides authority for this Court to order Apple to assist with the execution of the search warrant on Feng's phone. The New York Telephone Co. framework imposes a rational limit on the scope of the All Writs Act: namely, that orders to third parties in furtherance of lawful warrants cannot impose unreasonable burdens on those parties. Id. at 172. Here, there is no such unreasonable burden, and the requested relief falls squarely within the purview of this Court's authority under the All Writs Act.

Courts have repeatedly upheld the use of the All Writs Act to require third parties to provide services, such as technical assistance, and perform actions to assist the government. See, e.g., New York Telephone Co., 434 U.S. at 161 (requiring phone company to provide facilities and technical assistance with pen register); Mountain Bell, 616 F.2d at 1129 (requiring phone company to provide information, facilities, and technical assistance to facilitate tracing order); In re Application of U.S. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder, 610 F.2d 1148, 1155 (3d Cir. 1979) (requiring phone company to provide information, facilities, and technical assistance to facilitate tracing order, including the installation and continual operation of "card drops and other mechanical or electrical devices" and performance of "manual tracing operations" even though "the

execution of a trace may require a more extensive and more burdensome involvement on the part of the phone company" than the execution of a pen register).[3]

Following New York Telephone Co., courts have issued All Writs Act orders in support of warrants in a wide variety of contexts. These circumstances include:

- Ordering a phone company to assist with a trap and trace device. See In re Application, 610 F.2d at 1155; Mountain Bell, 616 F.2d at 1129.
- Ordering a phone company to produce telephone toll records. See United States v. Doe, 537 F. Supp. 838, 840 (E.D.N.Y. 1982); United States v. X, 601 F. Supp. 1039, 1042 (D. Md. 1984).
- Ordering a credit card company to produce customer records. See United States v. Hall, 583 F. Supp. 717, 722 (E.D. Va. 1984).
- Ordering a landlord to provide access to security camera videotapes. See Access to Videotapes, 2003 WL 22053105, at *3.
- Ordering a phone company to assist with consensual monitoring of a customer's calls. See In re Application, 2015 WL 5233551, at *4-5.

---

[3] Private parties have also benefited from the use of the All Writs Act to require third parties to assist in the execution of court orders. For example, in a case involving individuals operating computer botnets that sought to steal identification information, personal security information, and money from the computers of Microsoft's customers through the misuse of Microsoft's Windows operating system and Internet Explorer software, Microsoft Corp. sought and obtained an injunction against the individuals to stop them from creating such botnets as well as an All Writs Act order from a court to direct third-party Internet registries and registrars to transfer the criminal botnets' domains to the control of Microsoft. See Microsoft Corp. v. John Does 1-39, No. 12-CV-1335, ECF No. 13 (E.D.N.Y. Mar. 19, 2012) (Kuntz, J.); id., ECF No. 49 (July 10, 2015) (Johnson, J.); Microsoft Corp. v. John Does 1-82, No. 13-CV-319, 2013 WL 6119242 (W.D.N.C. Nov. 21, 2013); Microsoft Corp. v. John Does 1-18, No. 13-CV-139, 2014 WL 1338677 (E.D. Va. Apr. 2, 2014); see also Google Inc. v. Rockstar Consortium U.S. LP, No. 13-5933, 2014 WL 8735114 (N.D. Cal. Oct. 3, 2014) (issuing letters rogatory pursuant to the All Writs Act and other statutes to compel the testimony and production of documents for use at a patent infringement trial involving Google Inc.).

Significantly, in this exact context, numerous federal judges around the nation, including in the Eastern District of New York, have found it appropriate to issue orders under the All Writs Act to direct Apple to assist in extracting data from an Apple device through bypassing the passcode in order to execute a search warrant. See, e.g., In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant, No. 14-MC-288, ECF No. 2 (E.D.N.Y. Mar. 10, 2014) (Pollak, M.J.) (issuing requested All Writs Act order); In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant, No. 13-MC-214, ECF No. 2 (E.D.N.Y. Mar. 14, 2013) (Wall, M.J.) (same); In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant, No. 12-MJ-1083, ECF No. 3 (E.D.N.Y. Nov. 30, 2012) (Pollak, M.J.) (same); In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant, No. 11-MJ-1276, ECF Nos. 5-6 (E.D.N.Y. Dec. 28, 2011 and Jan. 9, 2012) (Gold, C.M.J.) (same); id., ECF No. 9 (E.D.N.Y. Jan. 23, 2012) (Pohorelsky, M.J.) (same); United States v. Navarro, No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013) (same); Hr'g Tr. at 8 (query of government prosecutors around the country revealed initial estimate of at least 70 prior All Writs Act orders to Apple); ECF No. 27 (identifying 13 additional instances in which courts across the country have issued similar All Writs Act orders during approximately the past five months); ECF No. 28 (listing one additional instance); Hr'g Tr. at 55 (counsel for Apple noting that it received All Writs Act orders with "frequency").

Courts that have further discussed the issue have explained that issuing such orders is appropriate under the All Writs Act and the precedent of New York Telephone Co. See In re [XXX], 2014 WL 5510865, at *1-3 (holding that All Writs Act relief "is appropriate to order the manufacturer here to attempt to unlock the cellphone so that the

warrant may be executed"); United States v. Blake, No. 13-CR-80054, ECF No. 207 at 5 (S.D. Fl. July 14, 2014) (holding that "the All Writs Act was properly invoked" to order Apple to provide password assistance and denying defendant's motion to suppress); see also Hr'g Tr. at 55-56 (counsel for Apple acknowledging that the routine issuance of All Writs Act orders indicated that "the weight of the authority" supported their issuance and "it seemed that this had been somewhat settled views and settled authority from multiple judges").

III. No Other Statute Limits the Application of the All Writs Act in this Case

As the Supreme Court has explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985) (emphasis added). Therefore, courts may not rely on the All Writs Act "[w]here a statute specifically addresses the particular issue at hand." Id.; New York Telephone Co., 434 U.S. at 172-73 (holding that federal courts may avail themselves of all auxiliary writs "unless appropriately confined by Congress"). This limitation has generally been interpreted to restrict a court's ability to issue All Writs Act relief where that specific relief is explicitly or implicitly prohibited by law. See, e.g., United States v. Barrett, 178 F.3d 34, 54-56 (1st Cir. 1999) (All Writs Act relief unavailable because § 2255 explicitly blocked petitioner's second post-conviction collateral attack); Pa. Bureau of Corr., 474 U.S. 34, 39-43 (All Writs Act relief unavailable because § 2243, by referring to transportation of prisoners by custodians, implicitly left out other parties such as the U.S. Marshals Service). There is no such express or implied prohibition in law here.

A. Current Law Does Not Specifically Address the Requested Relief

There is no statute that specifically addresses the procedures for requiring any device manufacturer, such as Apple, to extract data from a passcode-locked phone. As set forth below, the statutes discussed herein simply do not address physical searches of devices pursuant to a search warrant.

1. CALEA

The Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (2012) and in scattered sections of 18 U.S.C.), imposes certain capability requirements on telecommunications carriers. 47 U.S.C. § 1002. Specifically, 47 U.S.C. § 1002(a)(1) requires telecommunications carriers to ensure that their systems have the capability to enable the government (pursuant to lawful authorization) "to intercept" wire and electronic communications; interception "encompasses only acquisitions contemporaneous with transmission," United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); see 47 U.S.C. § 1001(1) (incorporating definition of "intercept" from the Wiretap Act, 18 U.S.C. § 2510(4)). CALEA exempts "information services" from the requirements it imposes on telecommunications carriers. 47 U.S.C. § 1002(b)(2).

CALEA further requires companies that service telecommunications carriers — namely, manufacturers of "telecommunications transmission and switching equipment" and "providers of telecommunications support services" — cooperate with telecommunications carriers so that they may meet these capability requirements. 47 U.S.C. §1005.

a. CALEA Does Not Apply to This Case

CALEA does not specifically address the present dispute for several reasons. CALEA does not regulate manufacturers of consumer devices. Apple, for purposes of this dispute, is a manufacturer of a consumer device. The government is seeking Apple's assistance because it manufactured Feng's phone, and Apple is uniquely able to offer that assistance because it manufactured Feng's phone.

CALEA regulates telecommunications carriers and related entities. Apple is not a telecommunications carrier. That term refers to a person or entity "engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." Id. § 1001(8)(A). It is also neither a manufacturer of "telecommunications transmission and switching equipment," nor a provider "of telecommunications support services." See, e.g., 47 U.S.C. §§ 1005, 1006(a). Indeed, Apple does not claim to fall within any of these definitions in this case and does not claim that it has any obligations under CALEA. ECF No. 20 at 1-2.

Apple is also not an "information service" for purposes of this application. While Apple notes that a "significant portion of [its] offerings are information services," it concedes that its "role as manufacturer of the iPhone" — i.e., the role relevant to this dispute — does not fall within CALEA's definition of information services. ECF No. 20 at 2.[4]

[4] The applicability of CALEA turns on the specific role that it plays in the given circumstances. See In the Matter of Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs., 20 F.C.C. Rcd. 14989, at ¶ 21 (2005) (analyzing CALEA obligations on a per-"component" basis), aff'd by Am. Council on Educ. v. F.C.C., 451 F.3d 226, 233 (D.C. Cir. 2006). Therefore, Apple's role in providing unrelated offerings, to which Judge Orenstein refers, is not relevant here.

Therefore, the exemption CALEA provides for information services does not speak to what is and is not required of Apple here.

Finally, § 1002 addresses telecommunications carriers' capabilities to access real-time communications and call-identifying information (i.e., data "in motion"). This case, however, involves access to data stored on a user device (i.e., data "at rest"). CALEA therefore has no application to this case.

b. CALEA's Limitations Section Does Not Prohibit the Relief Sought Here

Despite the fact that CALEA does not govern device manufacturers such as Apple or apply to data at rest on a user device like the data stored on Feng's phone, the magistrate judge nevertheless suggests that "it is arguable that CALEA explicitly absolves a company like Apple of any responsibility to provide the assistance the government seeks here" by way of the three subsections of the statute's "Limitations" section, codified in § 1002(b). ECF No. 29 at 15-17. By their very terms, the subsections within the Limitations section are entirely inapposite to the matter at hand.

The magistrate judge cites Section 1002(b)(1), which states that CALEA "does not authorize any law enforcement agency or officer" to require a "specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services" or "prohibit the adoption of any equipment, facility, service, or feature" by those same entities. Apple is not a manufacturer of telecommunications equipment, a provider of telecommunications support services, or a provider of a wire or electronic communication

service insofar as it pertains to this case. In any event, the government is not seeking to mandate any specific design or to prohibit the adoption of any equipment, facility, service, or feature by Apple. Subsection 1002(b)(1) therefore has no relevance to this dispute.

The magistrate judge also cites Section 1002(b)(2), which exempts "information services" from the capability requirements that apply to telecommunications carriers. As discussed above, Apple is not an "information service" as relevant to this dispute. Furthermore, Apple already has the technical capability to provide the requested relief. Subsection 1002(b)(2) therefore has no relevance to this dispute.

Finally, the magistrate judge cites Section 1002(b)(3), which provides that "[a] telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." This section is inapposite because, again, Apple is not a telecommunications carrier and, in any event, the proposed order does not require decryption. See Proposed Order at 2 ("Apple is not required to attempt to decrypt" data). Subsection 1002(b)(3) therefore has no relevance to this dispute.

2. Other Potentially Relevant Statutes

The Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.), also does not specifically address the present dispute because it also pertains to a different category of electronic information and does not regulate companies like Apple in their capacity as device manufacturers. Firstly, ECPA is directed to electronic communication services and remote computing services. 18 U.S.C. §§ 2510(15), 2711(2). Apple, as a

device manufacturer, is neither here. Thus, ECPA does not address the duty of Apple to assist in extracting data from an iPhone. Secondly, ECPA's Stored Communications Act addresses the means of preserving and obtaining user data stored in the servers of third-party providers (e.g., phone companies that provide cell phone service). This case, however, involves obtaining user data stored on the user's own device (i.e., Feng's phone). Courts have uniformly agreed that ECPA does not apply to end-user devices. See, e.g., Steiger, 318 F.3d at 1049 (holding that hacking into a home computer does not implicate ECPA because home computer is not an electronic communication service); Garcia v. City of Laredo, 702 F.3d 788, 792 (5th Cir. 2012) (holding that text messages and photos stored on cell phone are not protected by § 2701 of ECPA). ECPA is directed to electronic communication services and remote computing services. 18 U.S.C. §§ 2510(15), 2711(2). Apple, as a device manufacturer, is neither here. Thus, ECPA does not address the duty of Apple to assist in extracting data from an iPhone.

In the same realm, the Wiretap Act and the Pen Register statute include provisions mandating third-party assistance with real-time communications (wiretaps and pen-traps). See 18 U.S.C. §§ 2518(4), 3124(a), (b). These statutes do not apply to obtaining data stored on a device pursuant to a search warrant.

Thus, neither CALEA nor ECPA nor any other statute "specifically addresses" — or even vaguely addresses — the precise issue at the heart of this case: the duty of device manufacturers, like Apple, to assist in extracting data stored on a user's device where there is a valid search warrant for the device.

B. There is No Comprehensive Scheme Implying Prohibition

There is likewise no comprehensive statutory scheme that implicitly precludes obtaining such relief under the All Writs Act. At present, the law in this area consists of an incomplete patchwork of statutes addressing various aspects of electronic evidence preservation and collection, but not the matter at hand.

The magistrate judge concluded that All Writs Act relief is unavailable when there exists a comprehensive legislative scheme regulating the relevant area of law, even when that scheme does not expressly or impliedly prohibit the relief sought pursuant to the All Writs Act. ECF No. 29 at 20. The Supreme Court has never interpreted the All Writs Act in this limiting way. To be sure, a handful of lower courts have taken this view. See Application of the U.S., 427 F.2d 639 (9th Cir. 1970) (precluding All Writs Act authority to compel third-party assistance where there was a comprehensive statutory scheme covering wire interceptions); In re Application of U.S. in Matter of Order Authorizing Pen Register, 538 F.2d 956 (2d Cir. 1976) (same); In re Application of the U.S. for an Order Authorizing the Use of a Pen Register, 407 F. Supp. 398 (W.D. Mo. 1976) (same). However, the Supreme Court, in overturning the Second Circuit, looked askance at that position. See New York Telephone Co., 434 U.S. at 177 n.25 (observing that the Ninth Circuit's refusal to infer All Writs Act authority "in light of Congress' silence in a statute which constituted a 'comprehensive legislative treatment of wiretapping'" was subsequently overruled by Congress and declining to infer that such authority was previously lacking).

Even if the interpretation of the All Writs Act posited by the magistrate judge were the law, CALEA is not, as he argues, "part of a larger legislative scheme that is so comprehensive as to imply a prohibition." ECF No. 29 at 15-16. The handful of piecemeal

legislation, described above, that does exist addresses topics different from the matter before this Court and does not constitute a comprehensive statutory scheme. The touchstone of a comprehensive statutory scheme is a framework so detailed and pervasive that it implies that Congress intended to leave no room for supplementation. Cf., e.g., Gonzalez v. Raich, 545 U.S. 1, 10 (2005) (finding existence of a comprehensive regulatory scheme where Congress expressly enacted self-titled "Comprehensive" legislation to consolidate various laws and simultaneously repealed others); Block v. Cmty. Nutrition Inst., 467 U.S. 340, 351 (1984) (preclusion applies when "the congressional intent to preclude . . . is 'fairly discernible' in the detail of the legislative scheme"); Arizona v. United States, 132 S. Ct. 2492, 2501 (2012) (preclusion applies when Congress's intent to effect exclusive governance "can be inferred from a framework of regulation 'so pervasive . . . that Congress left no room'" for supplementation). The combination of CALEA and the ECPA is a far cry from the type of legislation that courts have found to constitute comprehensive schemes with preclusive or preemptive effect.

The best that can be said about the relevance of CALEA to this dispute is that it regulates entities and issues that are tangentially related to those at issue in this case. The mere presence of other statutes in the same realm however, does not preclude All Writs Act relief. For example, when the Court decided New York Telephone Co. in 1977, Congress had enacted Title III authorizing the real-time interception of the contents of communications, but it had not yet enacted the closely-related Pen Register statute for the real-time acquisition of non-content information. See Electronic Communications Privacy Act of 1986 § 301, 100 Stat. 1848 (enacting Pen Register statute). Despite the existence of a statute regulating government access to information closely related to pen registers, but not

specifically addressing pen registers, the Supreme Court held that an All Writs Act order could be issued in support of a warrant for a pen register.

This piecemeal legislation indicates Congress's incremental approach to legislating in this area, rather than Congress's intent to comprehensively legislate. As technology has changed, Congress has responded with new legislation addressing specific investigatory techniques, but it has never attempted to anticipate all eventualities in a field driven by rapid technological change. Meanwhile, the specific relief sought herein has consistently been left to the discretion of the federal courts, to decide on a case-by-case basis, under their All Writs Act authority. See cases cited supra at 17-18**.** The Court's residual authority under the All Writs Act is particularly important in an area like this, where legislation inevitably lags behind technology or risks obsolescence. In light of this statutory background, and consistent with New York Telephone Co., the All Writs Act continues to empower this Court to order third-party assistance to effectuate a search warrant.

C. Unenacted Proposals Do Not Override the Established Law of the All Writs Act

Given that Congress has not specifically addressed the relief sought herein, much less explicitly or implicitly prohibited that relief, there is no basis for concluding that the sought relief is anything other than "agreeable to the usages and principles of law." The absence of any express or implied prohibition of the requested relief in current law should end the matter. However, Judge Orenstein formulated what amounts to an unprecedented new limit to the Court's power in concluding that All Writs Act relief is also precluded where Congress has merely "considered and decided not to enact" a law conferring the requested authority. ECF No. 29 at 30. In effect, he uses opinions expressed by members of

Congress, divorced from the actual passage or rejection of legislation, to divine what "the usages and principles of law" are for purposes of the All Writs Act. This novel precept, that the actions and opinions of legislators — even when not connected with the passage of legislation — bear relevance to the interpretation of statutes passed centuries before the actions were taken and the opinions expressed, must be rejected.

As the Supreme Court has made perfectly clear, "unenacted approvals, beliefs, and desires are not laws." Puerto Rico Dep't of Consumer Affairs v. Isla Petroleum Corp., 485 U.S. 495, 501 (1988) (emphasis added). The reasons for this longstanding rule are obvious: firstly, the Constitution prescribes bicameralism and presentment — not the transcripts of congressional debates — as the voice by which the legislature may speak. U.S. Const. art. I. Under Article I, Congress speaks with legal force only when it speaks as one body, through bicameralism and presentment, i.e., when it passes a law. See I.N.S. v. Chadha, 462 U.S. 919, 946 (1983) (noting that bicameralism and presentment "are integral parts of the constitutional design for the separation of powers"). Secondly, "Congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction." Zino Davidoff SA v. CVS Corp., 571 F.3d 238, 243 (2d Cir. 2009) (quoting Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164, 187 (1994)); United States v. Craft, 535 U.S. 274, 287 (2002). There are many possible explanations for Congress's failing to pass laws in a given area, including that Congress is satisfied with existing authorities, or that Congress has not yet reached agreement on whether or how much to expand existing authorities, or that political considerations render legislating on a certain topic difficult at a given moment in time. It "is so often impossible to discern what the Members of Congress intended except to the extent that intent is manifested in the

only remnant of 'history' that bears the unanimous endorsement of the majority in each House: the text of the enrolled bill that became law." ACLU v. Clapper, 785 F.3d 787, 807-08 (2d Cir. 2015) (emphasis in original) (internal quotation marks omitted).

Judge Orenstein notes the longstanding rule precluding giving persuasive effect to Congressional inaction, but evades its effect in this case by expanding the definition of "Congressional action" to include activities short of the successful passage of a bill — activities that have traditionally been considered Congressional inaction. He holds that bills that have been introduced, but never even voted upon, are entitled to preclusive legal effect.[5] This approach has no basis in law, and Judge Orenstein cites none.[6] To the contrary, "Congress cannot express its will by a failure to legislate. The act of refusing to enact a law (if that can be called an act) has utterly no legal effect, and thus utterly no place in a serious discussion of the law." United States v. Estate of Romani, 523 U.S. 517, 535-36 (1998) (Scalia, J., concurring); see also Bowsher v. Synar, 478 U.S. 714, 733-34 (1986). Indeed, the Supreme Court has held that All Writs Act authority persists in the face of contemporaneous hearings and bills that do not result in law. The Supreme Court explained in such circumstances:

> Congress neither enacted nor rejected these proposals; it simply did not act on them. Even if it had, the legislation as proposed would have had no effect whatever on the power that Congress

---

[5] Judge Orenstein states that he would give preclusive legal effect even to bills that have been expressly rejected by veto. ECF No. 29 at 25 n.22.

[6] Judge Orenstein notes that the Supreme Court in New York Telephone Co. considered, in its analysis, "more recent congressional actions." ECF No. 29 at 24 n.21 (internal quotation marks omitted). However, as that case and the other three cases the magistrate judge relies on make clear, the Congressional "actions" considered were duly enacted laws, not neglected bills. Id.

> granted the courts by the All Writs Act. We cannot infer from the fact that Congress took no action at all . . . that Congress thereby expressed an intent to circumscribe traditional judicial remedies.

F.T.C. v. Dean Foods Co., 384 U.S. 597, 600, 609-10 (1966).

Moreover, by redefining activities that would normally be considered Congressional inaction as action, the magistrate judge is then able to give effect to legislative history that does not even accompany legislation. It is doubtful that any other court would agree that the legislative history of a bill that was never voted on could be used to interpret any statute, much less a statute passed hundreds of years earlier. See, e.g., Mead Corp. v. B.E. Tilley, 490 U.S. 714, 723 (1989) (even where considering subsequently enacted legislation, "[w]e do not attach decisive significance to the unexplained disappearance of one word from an unenacted bill because mute, intermediate legislative maneuvers are not reliable indicators of congressional intent" (internal quotations omitted)).

Judge Orenstein finds a home for this novel approach in the All Writs Act's requirement that writs be "agreeable to the usages and principles of law" by incorrectly stating that current federal case law "offers little if any guidance on how to understand that term in the context of this case." ECF No. 29 at 14. In fact, the Supreme Court has already explained that the phrase refers to the collection of historical writs that formed the basis of English and early American legal systems. In Bank of the United States v. Halstead, 23 U.S. 51 (1825), the Court explained:

> The precise limitations and qualifications of this power, under the terms, agreeable to the principles and usages of law, is not, perhaps, so obvious. It doubtless embraces writs sanctioned by the principles and usages of the common law. But it would be too limited a construction, as it respect writs of execution, to restrict it to such only as were authorized by common law. It

> was well known to Congress, that there were in use in the State Courts, writs of execution, other than such as were conformable to the usages of the common law. And it is reasonable to conclude, that such were intended to be included under the general description of writs agreeable to the principles and usages of law.

Id. at 56 (concluding that the All Writs Act authorized common law writs, state court writs, and any additional writs the courts deem appropriate, including the writ of venditioni exponas that was at issue in that case); see also United States v. Hayman, 342 U.S. 205, 221 n.35 (1952) (in "determining what auxiliary writs are 'agreeable to the usages and principles of law,' we look first to the common law"); Rawlins v. Kansas, 714 F.3d 1189, 1196 (10th Cir. 2013) (concluding that, under the All Writs Act, the court lacked jurisdiction to issue a writ of coram nobis because doing so in those circumstances was not "agreeable to the usages and principles of law"). As Judge Orenstein conceded, "Apple does not object that the type of assistance the government seeks here cannot find a close enough antecedent in the common law." ECF No. 29 at 14 n.10. Therefore, if the phrase "agreeable to the usages and principles of law" were interpreted according to the Supreme Court's instruction in Halstead, there would be no dispute between the parties that the writ sought herein was so agreeable.

Moreover, the magistrate judge's new interpretation of what courts are permitted to do under the Act runs directly contrary to this established precedent: the Supreme Court clearly stated that courts are free to "make additions" to and thereby "enlarge the effect and operation of the process" of the All Writs Act "to meet whatever changes might take place." Halstead, 23 U.S. at 60-62. It further held that doing so does not undermine the Constitutional safeguard of separation of powers because the All Writs Act merely gives power "to the Courts over their process" and "partakes no more of legislative

power than that discretionary authority in trusted to every department of the government"; and that, in any event, "should this trust not be duly and discreetly exercised by the Courts, it is at all times in the power of Congress to correct the evil by more specific legislation." Id.; see also Beers v. Haughton, 34 U.S. 329, 360 (1835) (recognizing Halstead's full consideration of the constitutional validity and extent of the courts' power and noting that "this delegation of power by congress [is] perfectly constitutional"). The magistrate judge, in his opinion, does not take into account this established case law. ECF No. 29 at 14 n.10.

Thus, the Supreme Court's opinion in Halstead fatally undermines the magistrate judge's novel interpretation of the All Writs Act because it makes clear that authority under the act to issue relief "agreeable to the usages and principles of law" imposes a relatively routine requirement on common law courts to abide the common usages of historical writs, not a radically new requirement that courts abide stray remarks and neglected proposals in Congress.

Even if the Court were to apply the novel interpretive gloss on the All Writs Act that Judge Orenstein advocates, there is no factual basis for finding that Congress considered and rejected the relief requested here.

The examples that Judge Orenstein relies upon do not pertain to the matter before this Court. They discuss amending CALEA to ensure that device manufacturers "build an access route" to data on their devices. See, e.g., ECF No. 2 at 3 (quoting law enforcement officer's testimony explaining that, in some cases, law enforcement can obtain lawful court orders to access data on devices but cannot carry out those orders where "the developer has not built the access route"). In this case, the access route already exists.

In this case, a valid warrant, seeking evidence in an ongoing investigation, remains unexecuted. There is a statutory gap to fill, and the Court is authorized under the All Writs Act to fill it. See New York Telephone Co., 434 U.S. 159 (using All Writs Act to compel third party assistance with a pen register prior to the passage of the Pen Register Statute). Exercising that authority here does not affect any ongoing congressional debate.

IV. The All Writs Act Provides this Court with the Authority to Issue the Order to Apple

In New York Telephone Co., the Supreme Court considered three factors in concluding that the issuance of the All Writs Act order to the phone company was appropriate. First, it found that the phone company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." 434 U.S. at 174. Second, it concluded that the order did not place an unreasonable burden on the phone company. Id. at 175. Third, it determined that the assistance of the company was necessary to achieve the purpose of the warrant. Id. As set forth below, each of these factors supports issuance of the order directed to Apple in this case.

A. Apple is Not Far Removed From This Matter

Apple is not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." Id. at 174. As in New York Telephone Co., the "Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis," and the company's noncompliance "threatened obstruction of an investigation which would determine whether the Company's facilities were being lawfully used." New York Telephone Co., 434 U.S. at 174.

Apple designed, manufactured, and sold the phone that is the subject of the search warrant, and Apple maintains strict control over what operating system software may run on that phone; namely, only operating system software designed and signed by Apple, i.e., iOS. Thus, Apple wrote and owns the software that is currently running on Feng's phone, and continues to maintain exclusive dominion over that software which is thwarting the execution of the warrant.[7]

Apple's software is actively impeding the execution of the search warrant in several ways. First, it includes the passcode feature that locks the phone and prevents government access to stored information without obtaining the correct passcode or a passcode-bypass. Second, it includes a remote wipe feature, activated on Feng's phone, that renders the data on the phone permanently inaccessible once the phone obtains a network connection. See "iCloud: Erase your device," https://support.apple.com/kb/PH2701 (last visited Mar. 2016), attached hereto as Exhibit G. Third, it includes an "auto-erase" feature which, if enabled by the user, renders the data on the phone inaccessible after multiple failed passcode attempts. See "Use a passcode with your iPhone, iPad, or iPod touch," Apple, https://support.apple.com/en-us/HT204060 (last visited Mar. 2016), attached hereto as Exhibit H. There is no way to know by examining the phone whether or not this function has

[7] Apple's software licensing agreement specifies that iOS 7 software is "licensed, not sold" and that users are merely granted "a limited non-exclusive license to use the iOS Software"; although users may make a "one-time permanent transfer of all" license rights, they may not otherwise "rent, lease, lend, sell, redistribute, or sublicense the iOS Software." See "Notices from Apple," Apple iOS Software License Agreement ¶¶ B(1)-(3), excerpts attached hereto as Exhibit E. Apple retains exclusive control over the software that can be used on iPhones; "only Apple-signed code can be installed on a device." See iOS Security at 5, Apple (Feb. 2014), attached hereto as Exhibit F.

been enabled. Accordingly, trying successive passcodes risks permanently losing access to the data on Feng's phone.

Apple has the ability to bypass the passcode and access the data on the phone without triggering the auto-erase feature, and has routinely done so for law enforcement agents who have obtained a search warrant and accompanying All Writs Act order. ECF No. 16 at 3. Apple's process for performing a passcode-bypass is proprietary to Apple: it has not shared its method with the government and the proposed order does not require that it do so. In this way, Apple retains the exclusive ability to safely access the contents of the phone and provides assistance to law enforcement only when it verifies that law enforcement has obtained lawful authority for such access.

In his opinion, Judge Orenstein concluded that Apple is too far removed to be compelled here. ECF No. 29 at 31. In support of that conclusion, the magistrate judge relied on the finding that to "the extent that Feng used his iPhone in committing crimes, he used his own property, not Apple's" — namely, the phone and the data on it — and did not "in any way use[] the licensed software itself" to facilitate his crimes. ECF No. 29 at 31, 32. To the contrary, Feng used Apple's property — the software on the phone — to commit and conceal his crimes. See Ex. C ¶¶ 9-28 (providing examples of Feng making and receiving phone calls to facilitate drug deals and explaining that there is probable cause to believe Feng also used other applications on the phone including contacts, call logs, chats, text messages, and photographs). As Apple itself has explained:

> The OS is the core operating software of the iPhone. It is responsible for handling the details of the operation of the device's hardware and for management and coordination of activities and operations that are necessary for the making and

> receiving of phone calls and for application programs (such as email and calendar) to execute on the device.

Responsive Comment of Apple Inc. In Opposition to Proposed Exemption 5A and 11A (Class #1) at 7, In re Exemption to Prohibition on Circumvention, No. RM 2008-8 (U.S. Copyright Office Feb. 2, 2009). Indeed, Apple's property — the software features including the passcode feature, auto-erase feature (if enabled), and remote wipe feature — continues to obstruct the investigation. Given that Apple manufactured, sold, and continues to exercise control over a phone used in a criminal enterprise, where it designed and has exclusive expertise about the software used to further that criminal enterprise, where that very software now thwarts the execution of the search warrant, and where Apple provides ongoing services to phone owners, including control over what software may run on the device and the ability to wipe the phone remotely, compulsion of Apple is permissible under New York Telephone Co.

Judge Orenstein also placed emphasis on the notion that Apple is not a "highly regulated public utility with a duty to serve the public." ECF No. 29 at 31-32 (internal quotation marks omitted). Law and precedent demonstrate that this factor is not dispositive. The All Writs Act, by its terms, does not limit the types of entities to which a writ may issue. While the Supreme Court in New York Telephone Co. noted that the telephone company in that case was a public utility, the Court also embraced the notion that a private citizen's "duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions." 434 U.S. at 175 n.24. In support of this proposition, the Court cited Babington v. Yellow Taxi Corp., 250 N.Y. 14, 17 (1928), a case not involving a public utility but rather a taxi driver who had been ordered by a police officer "to chase another

car." In doing so, the Court emphasized the more general proposition that it is neither improper nor unusual to expect civilians to assist law enforcement. See also Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 389 (6th Cir. 1977) (noting that at "common law a sheriff could require an unwilling citizen to assist him in executing king's writs, effecting an arrest, quelling riots and apprehending robbers"). Indeed, lower courts have not hesitated to direct All Writs Act orders to private individuals and businesses (that were not public utilities) to effectuate warrants. See Hall, 583 F. Supp. at 722 (credit card company); Access to Videotapes, 2003 WL 22053105, at *3 (landlord).

Judge Orenstein also observed that Apple was not involved in distributing methamphetamine with Feng or conspiring with Feng to obstruct justice. ECF No. 29 at 32 (Apple was not dealing drugs); id. at 35 (not conspiring); id. at 33 ("Apple had no involvement in Feng's crime, and it has taken no affirmative action to thwart the government's investigation of that crime"). To be clear, the government is not accusing Apple of criminal conduct in this case, nor is any such accusation relevant to the relief the government seeks. The Supreme Court has expressly held that even innocent third parties — persons who are "not . . . engaged in wrongdoing" and "have not taken any affirmative action to hinder justice," but are nevertheless "in a position to frustrate the implementation of a court order" — can be compelled to assist law enforcement under the All Writs Act. New York Telephone Co., 434 U.S. at 174.

Judge Orenstein found that "Apple is not doing anything to keep law enforcement agents from conducting their investigation," "has not barred the door to its property to prevent law enforcement agents from entering and performing actions they were otherwise competent to undertake in executing the warrant for themselves," and is "merely

declining to offer assistance." ECF No. 29 at 34-36. However, Apple's exclusive control over the software that can run on the phone, including its auto-erase feature, is the technological equivalent to barring the door. It prevents law enforcement agents from attempting to determine the passcode and perform the search themselves, without Apple's assistance. This is precisely the sort of frustration of a court order that warrants All Writs Act relief. Cf. New York Telephone Co., 434 U.S. at 162-63 (company that controlled telephone lines and "refused to lease lines . . . needed to install the pen registers in an unobtrusive fashion" could be compelled to assist law enforcement).

B. The Order Does Not Place an Unreasonable Burden on Apple

In addition, the proposed order does not place an unreasonable burden on Apple.

It is important to note that Apple has conceded this point: the company stated in public court filings in this case that if the Court issues the proposed order, it "would not likely place a substantial financial or resource burden on Apple." ECF No. 11 at 3 & n.3. Indeed, Apple has previously bypassed passcode-locked devices in response to court orders on numerous occasions, and has represented that the process takes only "several hours." Hr'g Tr. at 25. It has never required compensation for doing so, despite the availability of reasonable reimbursement under the law. Id. at 58. Furthermore, the company has conceded that the proposed order would not "infringe Apple's proprietary interests." Id. at 25.

Apple also admits that compliance with any lawful order issued in this case would not pose any reputational burden or harm to its customer trust. Id. at 60 (counsel for Apple acknowledging that if there is "sufficient basis in law" to require Apple's assistance,

"then [such assistance] wouldn't undermine customer trust").[8] Indeed, Apple continues to inform its customers that it can extract data from pre-iOS 8 devices, like this one, in response to law enforcement requests. See Ex. D, § III(I).

Where, as here, compliance with the order would not require inordinate effort, and reasonable reimbursement for that effort is available, no unreasonable burden can be found. See New York Telephone Co., 434 U.S. at 175 (holding that the All Writs Act order was not burdensome because it required minimal effort by the company, provided for reimbursement, and did not disrupt its business operations).

Courts have relied on the All Writs Act to mandate third-party assistance with search warrants in circumstances far more burdensome than what is requested here. For example, in Mountain Bell, 616 F.2d 1122, the United States obtained an All Writs Act order in support of a search warrant requiring the phone company to trace calls to specified phone numbers. Although the phone company complained that the order imposed a "serious drain upon existing personnel and equipment" over a 20-day period, and that the order "increased the likelihood of system malfunctions while at the same time impairing the company's ability to correct such problems," the Ninth Circuit rejected the phone company's argument that the order imposed an unreasonable burden.

Despite Apple's concessions and its long track record of providing law enforcement assistance without any discernible disruption of business operations, Judge

---

[8] While Apple previously expressed concern over harm to Apple's brand, that concern was based on enabling improper access to customer data. However, this is not a case of improper access: the government has a valid warrant to search the data on Feng's phone and, as explained above, this Court has clear legal authority to require Apple to assist in enabling that search.

Orenstein, remarkably, concluded that the proposed order would impose an unreasonable burden on Apple. ECF No. 29 at 45. The record is clear: Apple concedes there is no substantial burden in this case. That should be the end of the matter, and All Writs Act authority should be exercised to effectuate the warrant.

Faced with Apple's concession regarding the lack of burden imposed on it by the proposed order, Judge Orenstein acknowledged that any burden in terms of diverted "man hours and hardware and software . . . . is not substantial" in this case. ECF No. 29 at 41. In finding burdensomeness, the magistrate judge improperly looked beyond this case: to the "at least 70 times" in the past where Apple has already complied with similar orders — without once raising any claim of burden; the "dozen more" cases in which orders have issued during the pendency of this matter — in which Apple has similarly made no claim of burden; and to cases where the government has sought a different type of relief than the one requested here (a type of relief that even Judge Orenstein admitted is "more burdensome" to that sought here). ECF No. 29 at 41, 44-45.

The magistrate judge cited no authority for the conclusion that in determining the degree of burden that an All Writs Act order places on a party, courts may consider other applications for similar orders in unrelated cases, or other applications for different orders in unrelated cases. The case law suggests otherwise. See, e.g., Ivey v. Haney, No. 92-C-6875, 1994 WL 401098, at *4 (N.D. Ill. July 29, 1994) (rejecting "floodgates" argument that issuance of writ "will lead to a tremendous wave of requests for similar writs" and noting that the issuance of a writ "must be based upon a case-by-case analysis"). Relying on unrelated applications to determine the burden posed by a particular All Writs Act application is especially troubling where no factual record has been developed regarding

those other applications and the party to whom the order is addressed has conceded that the instant application would not be burdensome so long as it otherwise meets the legal standard. The Supreme Court, in reversing the Second Circuit, specifically rejected the notion that speculation over the issuance of writs in other cases "without limitation" should bar the issuance of a writ in the case at hand. See New York Telephone Co., 434 U.S. at 171-72, reversing Application of U.S., 538 F.2d at 962-63 (declining to issue writ based on speculation about "the future orders it spawns").

Judge Orenstein also held that a company's desire to "maintain congenial relations with the public" and its "private interest in commercial success" are cognizable burdens and incorporated such burdens that are "harder to quantify" into his analysis. ECF No. 29 at 40 n.35, 45. However, both New York Telephone Co. and Mountain Bell show that these concerns are not sufficient to establish an unreasonable burden under the All Writs Act. In both, the phone companies made arguments similar to those made by Apple. In New York Telephone Co., the company emphasized that it had "a long-standing policy of fostering the privacy of communications" and that "[p]rotection of this privacy is fundamental to the telephone business." Brief of N.Y. Tel. Co. at 2, New York Telephone Co., 434 U.S. 159 (1977) (No. 76-835), 1977 WL 189311, at *1. Similarly, in Mountain Bell, the phone company argued that use of the All Writs Act could jeopardize "continued public confidence" and that the "telephone communications system in this country cannot continue to operate well if the public perceives telephone companies and their employees as law enforcement agents who may at any time be conducting unobtrusive searches." See Brief of Mountain States Tel. Co. at 33, Mountain Bell, 616 F.2d 1122 (9th Cir. 1980) (No. CA 78-2366). Despite these protests, the Supreme Court and the Ninth Circuit held that

compliance did not impose an unreasonable burden. New York Telephone Co., 434 U.S. at 175; Mountain Bell, 616 F.2d at 1132.

C. Apple's Assistance is Necessary to Effectuate the Warrant

Third, orders issued under the All Writs Act must be "necessary or appropriate in aid of their respective jurisdictions." 28 U.S.C. § 1651(a). In New York Telephone Co., the Court held that its order met that standard because "[t]he provision of a leased line by the Company was essential to the fulfillment of the purpose — to learn the identities of those connected with the gambling operation — for which the pen register order had been issued." 434 U.S. at 175. The proposed All Writs Act order in this matter also meets this standard, as it is essential to ensuring that the government is able to perform the search ordered by the warrant.

The government does not have any adequate alternatives to obtaining Apple's assistance. The government could attempt to guess the phone's passcode, but multiple failed guesses could trigger Apple's auto-erase feature which, if enabled, would render the contents of the phone permanently inaccessible. There are 10,000 possible passcodes, and the auto-erase feature triggers after ten failed guesses. The government has explored the possibility of using third-party technologies but has determined that using such technology on Feng's phone presents the same risk of triggering the auto-erase feature. The government has asked Feng to provide the passcode voluntarily; Feng asserts, however, that he has forgotten the passcode, which renders him unable to offer assistance.

Apple agrees that the assistance it provides is unique and proprietary. There is no "easy mechanism by which Apple can disclose to the government the method of access" because the "way the system is configured, it requires certain authentication from [Apple's]

servers." Hr'g Tr. at 63. That is why the government seeks the type of assistance embodied in the proposed order, whereby the government will provide Apple with Feng's phone, Apple will use its proprietary technique to extract data from the phone, and then Apple will return the phone and a copy of the data to the government.

Judge Orenstein, in his opinion, agrees that if it is true that the government cannot adequately search Feng's phone without Apple's assistance, the necessity requirement is satisfied. ECF No. 29 at 45. The magistrate judge, however, perceives that there is "conflicting evidence in the record" about the availability of third-party technologies that could be used to circumvent the passcode on Feng's phone without Apple's assistance. ECF No. 29 at 46. Specifically, the magistrate judge finds that the government has made three inconsistent statements over two cases: that it "cannot bypass the passcode security of an Apple iPhone," that it can, and that it depends. ECF No. 29 at 46-47. The government takes this opportunity to clarify the record.

First, the government has never claimed that it cannot bypass the passcode of every Apple iPhone without Apple's assistance or that "that it is impossible for it to bypass the security of an earlier operating system without Apple's help." ECF No. 29 at 46-48. The government asserted, in its application to the magistrate judge, that it could not bypass the passcode of the specific phone in this case and that attempting to do so, "without Apple's assistance, if it is possible at all, would require significant resources and may harm the iOS device." See ECF No. 1 at 1-3 (noting that the DEA "has in its possession an iOS device" which "agents have tried to unlock . . . but have failed" and identifying the device by exhibit number, IMSI number, and telephone number).

Second, the government asserted, in another case in this district, United States v. Djibo, No. 15-CR-88, ECF No. 27 (E.D.N.Y. 2015), that it had bypassed the passcode security of certain other Apple iPhones using a third-party technology, and that it could have bypassed the passcode security of the specific phone in that case with the same technology. The argument in Djibo was hypothetical because, in the particular facts of that case, the agents had obtained the passcode and therefore did not need to perform a passcode-bypass. Tr. of Suppression Hr'g, Djibo, No. 15-CR-88, ECF No. 65 at 11. The testimony of the government's agent in Djibo was consistent with the government's position here: he testified that the technology is "not a forensic tool" but rather a "hacking tool," that it is "very finicky," and that it has had "varied success" with respect to particular iPhones which he identified by their model of hardware and software. Djibo Hr'g Tr. at 17-18, 28-29. To the extent that the government's briefing or oral argument in Djibo suggested that this third-party technology could be used to bypass the passcode security of any and all iPhones, regardless of the type of hardware and software, or that the government would have been willing to run the risk of activating the auto-erase feature regardless of the risk of data destruction, it was an overstatement and is hereby corrected and clarified.

Third, the government further explained, in this case, that the government's ability to bypass the passcode of an Apple iPhone is highly device-specific, and depends in part on the specific hardware and software in place. ECF No. 21 at 7-8. The government also explained that it had consulted with the testifying agent in Djibo and the agents in this case and determined that use of the third-party technology on the specific phone in this case could activate the auto-erase feature, if enabled, and render the data in the phone permanently inaccessible. Id.

As a result, in this case, the government cannot adequately search Feng's phone without Apple's assistance. Thus, and for all the foregoing reasons, an All Writs Act order directed to Apple is essential to facilitate execution of the warrant, and the necessity requirement of New York Telephone Co. is satisfied in this case.

All three New York Telephone Co. factors are therefore satisfied, and this Court should issue the All Writs Act order to Apple.

* * *

Judge Orenstein makes several additional points over the course of his opinion and the government need not address every point here. It focuses on those that are material to the analysis before this Court, which, in any event, is reviewing the matter de novo. The government notes, however, that much of Judge Orenstein's reasoning appears to be driven by a forward-looking concern for preventing future government abuse. See, e.g., ECF No. 29 at 32 n.26 (expressing concern over "a virtually limitless expansion of the government's legal authority to surreptitiously intrude on personal privacy"); id. at 27 (expressing concern for the "protection against tyranny"); id. at 18 n.14, 34-43. Judge Orenstein also appears to worry that, granting the specific relief requested in this case would compel the same ruling in other courts, in other cases, despite varying facts and circumstances and the discretionary nature of All Writs Act relief. Id. at 28. These concerns go far afield of the present case, and the Supreme Court has rejected using speculation about future harm as a basis to bar relief in a specific case. There is no basis for the Court to predict that the grant of the specific relief sought in this case — which has been previously granted in dozens of cases — would open the floodgates to different relief being granted in different cases, and no reason for this Court to rely on such a prediction to limit its own well-established All Writs Act authority.

In this case, the government arrested a criminal. The government got a warrant to search the criminal's phone. Law enforcement agents tried to search the phone themselves, but determined they could not do so without risking the destruction of evidence. The government then applied for a second court order to ask Apple to perform a simple task: something that Apple can easily do, that it has done many times before, and that will have no effect on the security of its products or the safety of its customers. This is how the system is supposed to work.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court grant the government's application and issue the proposed order.

Dated: Brooklyn, New York
March 7, 2016

Respectfully submitted,

ROBERT L. CAPERS
United States Attorney

By: /s/
Saritha Komatireddy
Lauren Howard Elbert
Ameet Kabrawala
Assistant U.S. Attorneys

Nathan Judish
Jared Hosid
Senior Counsel
Computer Crime and
Intellectual Property Section
Department of Justice
(Of Counsel)

cc: Clerk of the Court (MKB) (by ECF)
All counsel of record (by ECF)

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THE COURT	Case No. 15-MC-1902 APPLICATION

INTRODUCTION

The United States of America, by and through Robert L. Capers, United States Attorney, and Lauren Howard Elbert, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Apple Inc. ("Apple") to assist in the execution of a federal search warrant by bypassing the lock screen of an iOS device, specifically, an Apple iPhone 5s.

FACTS

The United States Drug Enforcement Administration ("DEA") currently has in its possession an iOS device that is the subject of a search warrant issued by this Court. The warrant is attached as an Exhibit. Inspection of the iOS device reveals that it is locked. Law enforcement agents have tried to unlock the telephone but have failed. Because the iOS device is locked, law enforcement agents are not able to examine the data stored on the iOS device as commanded by the search warrant.

The iOS device is an iPhone 5s labeled DEA Exhibit N-67, with IMEI number 013888005800316, IMSI number 310260572923753, and telephone number (908) 463-3333.

Apple, the creator of the iOS operating system and producer of the iOS device, may be capable of retrieving data stored on the iOS device that is not currently accessible to

DEA because the iOS device is locked. This Application seeks an order requiring Apple to use any such capability, so as to assist agents in complying with the search warrant.

DISCUSSION

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice… and 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). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Under the reasoning of *New York Tel. Co.*, this Court has the authority to order Apple to use any capabilities it may have to assist in effectuating the search warrant.

The government is aware, and can represent, that in other cases, courts have ordered Apple to assist in effectuating search warrants under the authority of the All Writs Act. Additionally, Apple has complied with such orders.

The requested order would enable agents to comply with this Court's warrant commanding that the iOS device be examined for evidence identified by the warrant. Examining the iOS device further without Apple's assistance, if it is possible at all, would require significant resources and may harm the iOS device. Moreover, the order is not likely to place any unreasonable burden on Apple.

Respectfully submitted,

Lauren Howard Elbert
Assistant United States Attorney
718-254-7577

Date: March 7, 2016

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THE COURT	Case No. 15-MC-1902 **ORDER**

Before the Court is the Government's motion for an order requiring Apple Inc. ("Apple") to assist law enforcement agents in the search of an Apple iOS device. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Apple assist law enforcement agents in the examination of the iPhone 5s labeled DEA Exhibit N-67, with IMEI number 013888005800316, IMSI number 310260572923753, and telephone number (908) 463-333 (the "IOS Device"), acting in support of a search warrant issued separately by this Court;

FURTHER ORDERED that Apple shall provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data ("Data") on the iOS Device;

FURTHER ORDERED that, to the extent that data on the iOS Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement, but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data;

FURTHER ORDERED that Apple's reasonable technical assistance may include, but is not limited to, bypassing the iOS Device user's passcode so that the agents may search the iOS Device, extracting data from the iOS Device and copying the data onto an external hard

drive or other storage medium that law enforcement agents may search, or otherwise circumventing the iOS Device's security systems to allow law enforcement access to Data and to provide law enforcement with a copy of encrypted data stored on the iOS Device; and

FURTHER ORDERED that although Apple shall make reasonable efforts to maintain the integrity of data on the iOS Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents.

To the extent that Apple believes that compliance with this Order would be unreasonably burdensome, it may make an application to this Court for relief within five business days of receipt of the Order.

Signed,

_____

THE HON. MARGO K. BRODIE
UNITED STATES DISTRICT JUDGE
EASTERN DISTRICT OF NEW YORK

Date: _____, 2016

EXHIBIT C

ABK
F.# 2014R00236

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

ONE WHITE SAMSUNG GALAXY S5 SMARTPHONE LABELED DEA EXHIBIT N-65;

ONE MOTOROLA SMARTPHONE LABELED DEA EXHIBIT N-66;

ONE APPLE IPHONE IN A GOLD-COLORED CASE LABELED DEA EXHIBIT N-67;

ONE SILVER-COLORED MOTOROLA CELLULAR TELEPHONE LABELED DEA EXHIBIT N-68;

ONE BLACK PALM CELLUAR TELEPHONE LABELED DEA EXHIBIT N-69;

ONE BLACK NOKIA CELLULAR TELEPHONE LABELED DEA EXHIBIT N-70;

ONE GRAY SAMSUNG GALAXY NOTE II SMARTPHONE LABELED DEA EXHIBIT N-71;

ONE BLACK ALCATEL CELLULAR TELEPHONE LABELED DEA EXHIBIT N-72;

ONE WHITE LG SMARTPHONE LABELED DEA EXHIBIT N-78; and

ONE BLACK SAMSUNG CELLPHONE LABELED DEA EXHIBIT N-84,

SEIZED ON OR ABOUT JUNE 11, 2014 FROM THE PREMISES LOCATED AT 41-21 149TH STREET, FIRST FLOOR, IN QUEENS, NEW YORK.

- X

15 M 0610

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

(Fed. R. Crim. P. 41)

EASTERN DISTRICT OF NEW YORK, SS:

BENJAMIN X. YU, being duly sworn, deposes and states that he is a Special Agent with the Drug Enforcement Administration ("DEA"), duly appointed according to law and acting as such.

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—namely, the above-referenced electronic devices described in Attachment A—which are currently in law enforcement possession in the Eastern District of New York, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration ("DEA"). I have been a DEA Special Agent for approximately 18 years and am responsible for investigating narcotics trafficking and money laundering, as well as other offenses. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. During my tenure with the DEA, I have participated in narcotics investigations during the course of which I have: (a) conducted physical and wire surveillance; (b) executed search warrants at locations where drugs, drug proceeds, records of narcotics, money laundering transactions and firearms have been found; (c) reviewed and analyzed numerous taped conversations and records of drug traffickers; (d) debriefed cooperating drug traffickers; (e) monitored wiretapped conversations of drug traffickers and

reviewed line sheets prepared by wiretap monitors; and (f) conducted surveillance of individuals engaged in drug trafficking and money laundering. Through my training, education, and experience, I have become familiar with (a) the manner in which illegal drugs are imported and distributed; (b) the method of payment for such drugs; and (c) the efforts of persons involved in such activity to avoid detection by law enforcement.

4. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. All referenced transcripts are in draft translation and form.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is as follows: ONE WHITE SAMSUNG GALAXY S5 SMARTPHONE LABELED DEA EXHIBIT N-65; ONE MOTOROLA SMARTPHONE LABELED DEA EXHIBIT N-66; ONE APPLE IPHONE IN A GOLD-COLORED CASE LABELED DEA EXHIBIT N-67; ONE SILVER-COLORED MOTOROLA CELLULAR TELEPHONE LABELED DEA EXHIBIT N-68; ONE BLACK PALM CELLUAR TELEPHONE LABELED DEA EXHIBIT N-69; ONE BLACK NOKIA CELLULAR TELEPHONE LABELED DEA EXHIBIT N-70; ONE GRAY SAMSUNG GALAXY NOTE II SMARTPHONE LABELED DEA EXHIBIT N-71; ONE BLACK ALCATEL CELLULAR TELEPHONE LABELED DEA EXHIBIT N-72; ONE WHITE LG SMARTPHONE LABELED DEA EXHIBIT N-78; and ONE BLACK SAMSUNG

CELLPHONE LABELED DEA EXHIBIT N-84, SEIZED ON OR ABOUT JUNE 11, 2014 FROM THE PREMISES LOCATED AT 41-21 149TH STREET, FIRST FLOOR, IN QUEENS, NEW YORK (collectively, the "DEVICES"). The DEVICES are in the custody of law enforcement officials in Brooklyn, New York.

6. The applied-for warrant would authorize the forensic examination of the DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On July 9, 2014, a grand jury empanelled in Eastern District of New York indicted the defendant, JUN FENG, also known as "KEVIN," and others, for conspiring to distribute and possessing with the intent to distribute a controlled substance containing methamphetamine, a Schedule II controlled substance, in violation of Title 21, United States Code, Sections 841(b)(1)(C) and 846. (See Docket No. 14-CR-387 (MKB)). The Indictment charges that the conspiracy occurred in or about and between approximately July 2013 and June 2014. The investigation is ongoing.

8. During the course of the investigation leading to the charges against FENG and others, law enforcement agents developed evidence indicating that FENG resided at 41-21 149th Street, First Floor, Queens, New York (the "Subject Premises") and used the Subject Premises to store and distribute controlled substances. On two occasions described below—February 27, 2014 and April 27, 2014—a distributor of crystal methamphetamine ("crystal meth") named HAN WOON NG ("NG") met with FENG at the Subject Premises

shortly before NG sold crystal meth to an agent acting in an undercover capacity (the "UC"); NG has also been indicted as part of the above-mentioned charged drug distribution conspiracy. On both occasions, surveillance and intercepted wire communications indicated that FENG was the source of the crystal meth and that NG obtained the crystal meth from FENG's residence, Subject Premises.

February 27, 2014 Crystal Meth Transaction

9. On February 27, 2014, the UC met with NG, a distributor of crystal meth. The UC asked NG whether NG could obtain crystal meth. NG suggested that they meet again later that day, at about 7:00 or 8:00 p.m., and made several telephone calls in the UC's presence.[1] Included among these calls was a call to FENG. The following is an excerpt of that call:

FENG:	Hello?
NG:	Hey, that, that, that, that…will you be able to get it? It's not, it's not, it's not the "Seafood." The other "Pork".
FENG:	"Pork"… How much do you need? The order that I asked yesterday is still not placed today.
NG:	I have not decided yet.

[1] All calls referenced in this Affidavit were lawfully recorded pursuant to court-authorized wiretaps. Not all relevant calls are described herein. Moreover, for those calls described, not all relevant portions of such conversations have been described. To the extent that quotations are used in the descriptions below, the quoted segments are based on draft line sheets and reviews of recordings and not final transcripts. Quoted passages include translations from Cantonese, Mandarin and Fujianese in draft form. Also, dates and times are approximate and based on the monitoring equipment at the time the call was intercepted.

FENG: It hasn't been deliver[ed] yet.

NG: I know. Will it be available tonight?

FENG: I don't know. How much stuff do you want to order?

NG: Right now, one quarter.

FENG: [UNINTELLIGIBLE]

NG: A quarter or a half.

FENG: It's better to take half. It's more worth it.

NG: I know that, but when will you have it? Today I need to tell him. I am with him right now at the shopping place.

FENG: Uh…okay. I will ask. I will call you when I am done with the phone call.

10. Based on my training, experience and familiarity with this investigation, I believe NG called FENG to discuss the acquisition of narcotics for the UC, using the code words "pork" and "seafood" to indicate different kinds of narcotics. NG also added that he wanted a "quarter" or a "half;" based on my training, experience and the investigation to date, I believe that the words "quarter" and "half" refer to a quarter ounce (7 grams) or a half ounce (14 grams), which are common weights in drug transactions.

11. After an additional call to FENG, NG left the UC and agreed to meet with the UC later that afternoon/evening. Over the next few hours, agents from the DEA surveiled NG as he drove to several different locations in Queens, New York, including the Subject Premises.

12. At approximately 7:30 p.m., after NG had visited and left the Subject Premises, NG and his associate and co-defendant SZE WONG TSUI ("TSUI") spoke on the

telephone to discuss transportation to the meeting site. The following is an excerpt of one of their conversations:

TSUI: What now?

NG: No, it's better to wait for you, better to wait for you. Better to wait for me.

TSUI: Wait for me again? Where are you?

NG: Deliver it there and I'll collect…collect the money.

TSUI: Where are you?

NG: Home. I'll wait for you at home.

TSUI: Ok, ok. Mm. Bye.

13. Shortly before 8 p.m. that evening, TSUI drove to NG's residence, picked up NG, and then drove NG to a Sheraton Hotel in Flushing, Queens to meet with the UC. Agents from the DEA surveiled the hotel and saw NG enter and exit the hotel while TSUI stayed in the car. Once he was inside the hotel, NG sold the UC approximately 8 grams of crystal meth.

14. The next day, February 28, 2014, FENG called NG. During this conversation, FENG asked NG, "So what did he say about the seafood that you brought over." Based on my training and experience and the investigation so far, I believe that FENG called NG because he was curious to learn what the UC thought of the narcotics that FENG had provided NG for the UC.

April 17, 2014 Crystal Meth Transaction

15. On April 17, 2014, at approximately 4:40 p.m., the UC, a cooperating witness ("CW") and NG met at the Sheraton Hotel in Flushing, Queens to negotiate an additional narcotics transaction. During the meeting, the UC requested two ounces of crystal meth. At approximately 6:05 p.m., NG left the hotel. A few minutes later, at approximately 6:13 p.m., NG called TSUI. The following is an excerpt of that conversation:

NG:	What's going on big brother Jimmy?
TSUI:	What?
NG:	Where are you?
TSUI:	I'm home, what now?
NG:	Nothing, I'm coming back home.
TSUI:	Fine, just come back.
NG:	I have something to be work on. I'm working on something. Motherfucker, If I should call "K".
TSUI:	What does it have to do with K?
NG:	Ah... Uncle Guai doesn't have that much. He doesn't have that much.
TSUI:	K doesn't have it.
NG:	He can't get it?
TSUI:	You can ask him, but I can tell you for sure that he doesn't have it.
NG:	Oh...

TSUI: If he tells you that he does have some, then he's slapping himself across the face because he was telling me he doesn't have any this whole time. Is he really that stupid?

NG: Then how come last time he said he has some? [LAUGHS]

TSUI: He told me he has none.

NG: Remember last time when I borrow three hundred dollars from you?

TSUI: Yeah.

NG: That's when I asked him to help me.

TSUI: Well, he told me he doesn't have any every time.

16. Based on my training, experience and the investigation to date, NG and TSUI were discussing whether "K,"—which I believe is short for "Kevin" (FENG's alias)—has narcotics to satisfy NG's order.

17. Once NG and TSUI finished their telephone call, NG immediately called FENG. The following is an excerpt of that conversation:

FENG: You can speak.

NG: Can you go out and do something?

FENG: What kind of thing do you want me to do? Is it "Pork"?

NG: I'm asking you to help me to do something. Actually it's better if I can come over in person and talk to you it's better.

FENG: I'm home.

NG: Okay, I can be there in two minute[s] at your home.

FENG: Yeah, okay.

18. Based on my training, experience and the investigation to date, NG and FENG again used the word "pork" as code for narcotics. Moreover, when NG said that he could "be there in two minutes[s] at your home," NG was referring to the Subject Premises. Then, a few minutes after NG and FENG completed their telephone call, agents surveiled NG as he arrived at the Subject Premises.

19. As with the prior transaction, after NG had visited and left the Subject Premises, NG and TSUI spoke on the phone to discuss transportation to the meeting site. Agents then observed TSUI and NG drive to the Sheraton Hotel. As they drove to the hotel, NG called FENG; the following is an excerpt of that telephone call:

NG: Uh, I'm on Parson and Roosevelt, on my way going down, (I'm) about to arrive.

FENG: Uh, you come to… You will be coming to 3370, right?

NG: 3370? I have to drive back again and turn around. That, that, those newspapers, newspapers are still over there.

FENG: Can't you just come over here?

NG: Me? He is there eating dinner. He…

FENG: Where?

NG: He's having dinner underneath the hotel.

FENG: Which hotel?

NG: That one, Sheraton, Sheraton.

FENG:	How far is it from Sheraton to over here?
NG:	I, I asked Brother Jimmy to drive.
FENG:	Okay.
NG:	Would it be a bit better if I waited for you at the parking lot?
FENG:	I'm afraid.
NG:	No, you go down only when you see me.
FENG:	Okay, fine.
NG:	No, you, you are not going to see him, only me.
	[VOICES OVERLAP]
FENG:	I, I won't see any one, all right?
NG:	Won't see anyone, of course, you certainly won't see anyone, okay? (You) will only see me. I'll go down to take care of it and will get back to give, give you the newspapers.
FENG:	Uh, fine, bye.

20. Based on my training, experience and the investigation to date, I believe that NG encouraged FENG to come to the hotel so that NG could give FENG "newspapers," which appears to be a code word for money. During this conversation, FENG expressed fear at the prospect of coming to the hotel but NG assured FENG that FENG wouldn't see anyone other than himself (NG).

21. Once NG, TSUI and FENG arrived at the Sheraton Hotel, agents surveiled NG as he walked over to FENG's vehicle and talked with FENG. NG then went

into the Sheraton Hotel alone. Once he was inside the hotel, NG gave the UC 42 grams of crystal meth in exchange for $4600.

22. Based on the foregoing, on June 6, 2014, the Honorable Marilyn D. Go, United States Magistrate Judge for the Eastern District of New York, issued a warrant authorizing the search of the Subject Premises. (See Docket No. 14-M-530.) Among other things, the June 6, 2014 search warrant authorized the seizure of cellular telephones and their stored information.

23. On or about June 11, 2014, law enforcement agents executed the June 6, 2014 search warrant on the Subject Premises. During their search, agents recovered, among other things, the DEVICES, together with suspected crystal methamphetamine, a bundled stack of United States currency, weighing devices, baggies, packaging material and other indicia of the sale, transportation and use of crystal meth.

24. Based on my training and experience, discussions with other law enforcement officers and my familiarity with this investigation, I understand that individuals involved in conspiracies to possess with intent to distribute narcotics often do not act alone and often communicate with co-conspirators by means of cellular telephones such as the DEVICES. They commonly maintain records that reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain records of communications such as call logs, chats and text messages in their cellular telephones. They also commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals often maintain these records of

communication and photographs in their possession and in their cellular telephones for a substantial period of time.

25. Further, based on my knowledge, training and experience, I know that the DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time. Even when deleted by the user, this information can sometimes be recovered with forensic tools.

26. Law enforcement authorities have made efforts to identify the particular device or devices used by FENG during the above-described calls. In particular, law enforcement authorities have subpoenaed records associated with the telephone number used by FENG during the above-described calls; the make and model of the telephone device(s) was specifically requested. Despite these efforts, to date, law enforcement authorities have been unable to identify the device(s) associated with the above-described calls.

27. The DEVICES are currently in the lawful possession of law enforcement authorities and were seized during the execution of the search warrant at the Subject Premises on June 11, 2014. Therefore, while the DEA might already have all necessary authority to examine the DEVICES, I seek this additional warrant out of an abundance of caution to be certain that an examination of the DEVICES will comply with the Fourth Amendment and other applicable laws.

28. Since their seizure, the DEVICES have been in sealed evidence bags in law enforcement custody. In my training and experience, I know that the DEVICES have

been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICES first came into the possession of the DEA. There is therefore probable cause to believe that the DEVICES contain evidence, fruits, and instrumentalities of federal narcotics trafficking offenses, including a conspiracy to distribute and possessing with the intent to distribute a controlled substance containing methamphetamine, a Schedule II controlled substance, in violation of Title 21, United States Code, Sections 841 and 846.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another

location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer device attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training, experience and research, I know that electronic devices such as the DEVICES have capabilities that allow them to serve wireless telephones, digital cameras, portable media players, GPS navigation devices, and/or PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have

been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICES were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer device is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

34. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

WHEREFORE, I respectfully submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the DEVICES described in Attachment A to seek the items described in Attachment B.

BENJAMIN X. YU
Special Agent
Drug Enforcement Administration

Sworn to before me this
6th day of July, 2015

THE HONORABLE VIKTOR V. POHORELSKY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The properties to be search are described as follows: ONE WHITE SAMSUNG GALAXY S5 SMARTPHONE LABELED DEA EXHIBIT N-65; ONE MOTOROLA SMARTPHONE LABELED DEA EXHIBIT N-66; ONE APPLE IPHONE IN A GOLD-COLORED CASE LABELED DEA EXHIBIT N-67; ONE SILVER-COLORED MOTOROLA CELLULAR TELEPHONE LABELED DEA EXHIBIT N-68; ONE BLACK PALM CELLUAR TELEPHONE LABELED DEA EXHIBIT N-69; ONE BLACK NOKIA CELLULAR TELEPHONE LABELED DEA EXHIBIT N-70; ONE GRAY SAMSUNG GALAXY NOTE II SMARTPHONE LABELED DEA EXHIBIT N-71; ONE BLACK ALCATEL CELLULAR TELEPHONE LABELED DEA EXHIBIT N-72; ONE WHITE LG SMARTPHONE LABELED DEA EXHIBIT N-78; and ONE BLACK SAMSUNG CELLPHONE LABELED DEA EXHIBIT N-84, SEIZED ON OR ABOUT JUNE 11, 2014 FROM THE PREMISES LOCATED AT 41-21 149TH STREET, FIRST FLOOR, IN QUEENS, NEW YORK (collectively, the "DEVICES"). This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the DEVICES described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846 and involve JUN FENG, also known as "KEVIN," and others, including:

   a. lists of customers and related identifying information;

   b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   d. any information recording the defendants' schedule or travel;

   e. any information recording the defendant communications with any co-defendant co-conspirator; and

   f. all bank records, checks, credit card bills, account information, and other financial records.

2. Records and evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, records, documents, and browsing history; and

3. Records evidencing the use of the Internet Protocol addresses, including:

   a. records of Internet Protocol addresses used;

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

EXHIBIT D

Legal Process Guidelines

U.S. Law Enforcement

These Guidelines are provided for use by law enforcement or other government entities in the U.S. when seeking information from Apple Inc. ("Apple") about users of Apple's products and services, or from Apple devices. Apple will update these Guidelines as necessary. This version was released on September 29, 2015.

All other requests for information regarding Apple users, including user questions about disclosure of information, should be directed to http://www.apple.com/privacy/contact/. These Guidelines do not apply to requests that law enforcement agencies make outside the U.S. to Apple's relevant local subsidiaries.

For government information requests, we comply with the laws pertaining to global entities that control our data and we provide details as legally required. For content requests from law enforcement agencies outside the U.S., with the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), Apple will only provide content in response to a search warrant issued pursuant to the Mutual Legal Assistance Treaty process or through other cooperative efforts with the United States Department of Justice.

INDEX

I. General Information

Apple designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store. User information is held by Apple in accordance with Apple's privacy policy and the applicable terms of service/terms and conditions for the particular service offering. Apple is committed to maintaining the privacy of the users of Apple products and services ("Apple users"). Accordingly, information about Apple users will not be released without proper legal process.

The information contained within these Guidelines is devised to provide information to law enforcement agencies regarding the legal process that Apple requires in order to disclose electronic information to law enforcement and government agencies. These Guidelines are not intended to provide legal advice. The frequently asked questions ("FAQ") section of these Guidelines is intended to provide answers to some of the more common questions that Apple receives. Neither these Guidelines nor the FAQ will cover every conceivable circumstance that may arise. Accordingly, please contact subpoenas@apple.com with any further questions. This email address is intended solely for use by law enforcement and government agents. If you choose to send an email to this address, it must be from a valid government email address. Nothing within these Guidelines is meant to create any enforceable rights against Apple and Apple's policies may be updated or changed in the future without further notice to law enforcement.

The majority of subpoenas, search warrants, and court orders that Apple receives seek information regarding a particular Apple device or customer and the specific service(s) that Apple may provide to that customer. Apple can provide Apple device or customer information in so far as Apple still possesses the requested information pursuant to its data retention policies. Apple retains data as outlined in certain "Information Available" sections below. All other data is retained for the period necessary to fulfill the purposes outlined in our privacy policy. Law enforcement should be as narrow and specific as possible when fashioning their legal process to avoid misinterpretation and/or objections in response to an overly broad request. Law enforcement is required to obtain a search warrant that is issued upon a probable cause showing for search warrants requesting user content.

II. Service of Process Guidelines

A. Service of Law Enforcement Subpoenas, Search Warrants, and Court Orders

Apple will accept service of subpoenas, search warrants, and court orders for information by email from law enforcement agencies, provided these are transmitted from the official email address of the law enforcement agency concerned. Law enforcement officers submitting a legal request to Apple should transmit it directly from their official law enforcement email address to the mailbox subpoenas@apple.com.

Please serve process in PDF format via an official law enforcement/government email address directly and exclusively to:

subpoenas@apple.com

Apple Inc.
Attention: Privacy and Law Enforcement Compliance
1 Infinite Loop, Cupertino, CA 95014

The above email address is intended solely for use by law enforcement and government agents. When law enforcement has served legal process on Apple by email to subpoenas@apple.com, in order to prevent disproportionate effort, there is no need to serve duplicate hardcopy process on Apple by mail.

We require law enforcement to include the following information with the legal request so the request can be verified:

Law Enforcement Agency
Law Enforcement Agent Name and Badge/ID number
Agency issued email address
Law Enforcement Phone number (with extension if applicable)
Verifiable physical return address
Law Enforcement Fax number

Note: All matters that are not law enforcement related must be either personally served at Apple's headquarters in Cupertino, California or served through CT Corporation (Apple's registered agent for service of process). For any inquiries related to law enforcement legal process, please contact: subpoenas@apple.com. If you are inquiring regarding the status of a specific subpoena, search warrant, or court order, please do not contact Apple until at least 10 business days after service of your request unless the matter involves imminent harm or threat to life.

B. Witness Testimony Subpoenas

Apple will not waive service requirements for subpoenas seeking witness testimony nor accept service via electronic means. All subpoenas seeking witness testimony must either be personally served on Apple or served through Apple's registered agent for service of process. Apple will resist subpoenas for witness testimony that are served with fewer than 14 days advance notice.

C. Preservation Requests

Requests to preserve information pursuant to 18 U.S.C. § 2703(f) should be directed to Apple's Privacy and Law Enforcement Compliance Group by email to subpoenas@apple.com. Please submit preservation requests on law enforcement letterhead with the agent and agency identified within the letter and include a valid government email address and phone number in the letter so the request can be verified.

Preservation requests must include the relevant Apple ID/account email address, or full name **and** phone number, and/or full name **and** physical address of the subject Apple account. When a

preservation request has been received, Apple will preserve a one-time data pull of the requested existing user data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended one additional 90-day period upon a renewed request. More than two preservations for the same account will be treated as requests for an extension of the originally preserved materials, but Apple will not preserve new material in response to such requests.

D. Emergency Disclosure

The Electronic Communications Privacy Act ("ECPA") covers the authorized disclosure of content by Apple. An exception to the requirement that law enforcement obtain a search warrant for customer content is provided by ECPA in situations in which the case involves an emergency. Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4) Apple is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay.

In order to request that Apple voluntarily disclose information on an emergency basis, please fill out the Emergency Law Enforcement Information Request form available at Appendix A and send a copy of the completed form by email to the mailbox: exigent@apple.com and include "Emergency Law Enforcement Information Request" in the subject line.

In the event that Apple produces customer data in response to an Emergency Law Enforcement Information Request, a supervisor for the law enforcement agent who submitted the Emergency Law Enforcement Information Request will be contacted and will be asked to confirm to Apple that the emergency law enforcement information request was legitimate. Apple requires that the law enforcement agent who submits the Emergency Law Enforcement Information Request provide the supervisor's contact information upon submission of the request.

If you need to contact Apple after hours (before 8:00 am or after 5:00 pm Pacific time) for an emergency inquiry, please contact Apple's Global Security Operations Center (GSOC) at (408) 974-2095.

E. Account Deletion Requests

In the event that law enforcement is requesting that Apple delete a customer's Apple ID, law enforcement is required to provide Apple with a court order or warrant specifying the account that is to be deleted and the basis for the request.

F. User Notice

Apple will notify its customers when their personal information is being sought in response to legal process except where providing notice is prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), or by applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.

Apple will provide delayed notice for emergency disclosure requests except where notice is prohibited by court order or applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment. Apple will provide delayed notice for requests after expiration of the non-disclosure period specified in a court order unless Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment.

III. Information Available From Apple

A. Device Registration

Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device prior to iOS 8 and OS Yosemite 10.10. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running OS Yosemite 10.10 and later versions is received when a customer associates a device to an iCloud Apple ID. This information may not be accurate or reflect the device's owner. Registration information can be obtained with a subpoena or greater legal process.

Please note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. Requests for serial numbers with either the letter "O" or "I" will yield no results.

B. Customer Service Records

Contacts that customers have had with Apple customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available. This information can be obtained with a subpoena or greater legal process.

C. iTunes

iTunes is a free software application which customers use to organize and play digital music and video on their computers. It's also a store that provides content for customers to download for their computers and iOS devices. When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections may also be available. iTunes subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. iTunes purchase/download transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific content purchased or downloaded.

D. Apple Retail Store Transactions

Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple Retail Store. A subpoena or greater legal process is required to obtain information regarding the type of card associated with a particular purchase, name of the purchaser, email address, date/time of the transaction, amount of the transaction, and store location. When providing legal process requesting Point of Sale records, include the complete credit/debit card number used and any additional information such as date and time of transaction, amount, and items purchased. Additionally, law enforcement may provide Apple with the receipt number associated with the purchase(s) in order to obtain duplicate copies of receipts, in response to a subpoena or greater legal process.

E. Apple Online Store Purchases

Apple maintains information regarding online purchases including name, shipping address, telephone number, email address, product purchased, purchase amount, and IP address of the purchase. A subpoena or greater legal process is required in order to obtain this information. When requesting information pertaining to online orders (excluding iTunes purchases), a complete credit/debit card number, an order number, reference number, or serial number of the item purchased. A customer name in combination with these parameters may also be provided, but customer name alone is insufficient to obtain information.

F. iTunes Gift Cards

iTunes gift cards have a sixteen-digit alphanumeric redemption code which is located under the "scratch-off" gray area on the back of the card, and a nineteen-digit code at the bottom of the card. Based on these codes, Apple can determine whether the card has been activated[1] or redeemed as well as whether any purchases have been made on the account associated with the card. When iTunes gift cards are activated, Apple records the name of the store, location, date, and time. When iTunes gift cards are redeemed through purchases made on the iTunes Store, the gift card will be linked to a user account. iTunes gift cards purchased through the Apple Online Store can be located in Apple systems by their Apple Online Store order numbers (note: this only applies to iTunes gift cards purchased through Apple as opposed to third-party retailers). Information regarding the customer who redeemed the cards will require a subpoena, and transactional information about iTunes purchases will require a court order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide specific iTunes content purchased.

Apple is unable to deactivate iTunes gift cards in response to legal process from a law enforcement/ government agency.

G. iCloud

iCloud is Apple's cloud service that allows users to access their music, photos, documents, and more from all their devices. iCloud also enables subscribers to back up their iOS devices to iCloud. With the iCloud service, subscribers can set up an iCloud.com email account. iCloud email domains can be

---

[1] Activated means that the card was purchased at a retail point-of-sale but not that it was used or redeemed (i.e., used to increase the store credit balance on an iTunes account or used to purchase content in the iTunes Store).

@icloud.com, @me.com[2] and @mac.com. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers.

iCloud is a subscriber based service. Requests for iCloud data must include the relevant Apple ID/ account email address. If Apple ID/account email address are unknown, Apple requires subscriber information in the form of full name **and** phone number, and/or full name **and** physical address to identify the subject Apple account.

The following information may be available from iCloud:

i. Subscriber Information

When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. Connection logs are retained up to 30 days.

ii. Mail Logs

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant. iCloud mail logs are retained up to 60 days.

iii. Email Content

iCloud only stores the email a subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. Apple is unable to provide deleted content. Available email content may be provided in response to a search warrant issued upon a showing of probable cause.

iv. Other iCloud Content. Photo Stream, Docs, Contacts, Calendars, Bookmarks, iOS Device Backups

iCloud only stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud content may be provided in response to a search warrant issued upon a showing of probable cause.

---

[2] iCloud has replaced the MobileMe service. Accordingly, Apple does not have any separate content associated with former MobileMe accounts. If the content is not in iCloud, it is no longer being stored.

H. Find My iPhone

Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device. More information about this service can be found at http://www.apple.com/icloud/find-my-iphone.html. Location information for a device located through the Find My iPhone feature is user facing and Apple does not have records of maps or email alerts provided through the service. Find My iPhone connection logs may be available and can be obtained with a subpoena or greater legal process. Find My iPhone connection logs are available for a period of approximately 30 days. Find My iPhone transactional activity for requests to remotely lock or erase a device may be available with an order under 18 U.S.C. § 2703(d) or a court order with the equivalent legal standard or a search warrant.

Apple cannot activate this feature on users' devices upon a request from law enforcement. The Find My iPhone feature must have been previously enabled by the user for that specific device. Apple does not have GPS information for a specific device or user.

I. Extracting Data from Passcode Locked iOS Devices

For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 through iOS 7. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party app data.

The data extraction process can only be performed at Apple's Cupertino, California headquarters for devices that are in good working order. For Apple to assist in this process, the language outlined below must be included in a search warrant, and the search warrant must include the serial or IMEI number of the device. For more information on locating the IMEI and serial number of an iOS device, refer to http://support.apple.com/kb/ht4061.

Please make sure that the name of the judge on the search warrant is printed clearly and legibly in order for the paperwork to be completed.

Once law enforcement has obtained a search warrant containing this language, it may be served on Apple by email to subpoenas@apple.com. The iOS device can be provided to Apple for data extraction either through an in person appointment or through shipment. If law enforcement chooses to ship the device, the device should not be shipped unless and until the officer receives an email from Apple requesting shipment.

For an in-person data extraction process, Apple requires that the law enforcement agent bring a FireWire hard drive with a storage capacity of at least two times the memory capacity for the iOS device. Alternatively, if law enforcement chooses to ship the device, law enforcement should provide Apple with an external hard drive or USB "thumb" drive with a storage capacity of at least two times the memory capacity for the iOS device. Please do not send the device unless and until you receive an email requesting its shipment.

After the data extraction process has been completed, a copy of the user generated content on the device will be provided. Apple does not maintain copies of any user data extracted during the process; accordingly all evidence preservation remains the responsibility of the law enforcement agency.

Required Search Warrant Language:

> "It is hereby ordered that Apple Inc. assist [LAW ENFORCEMENT AGENCY] in its search of one Apple iOS device, Model #_____, on the _____ network with access number (phone number) _____, serial[3] or IMEI[4] number _____, and FCC ID#_____ (the "Device"), by providing reasonable technical assistance in the instance where the Device is in reasonable working order and has been locked via passcode protection. Such reasonable technical assistance consists of, to the extent possible, extracting data from the Device, copying the data from the Device onto an external hard drive or other storage medium, and returning the aforementioned storage medium to law enforcement. Law Enforcement may then perform a search of the device data on the supplied storage medium.
>
> It is further ordered that, to the extent that data on the Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data.
>
> Although Apple shall make reasonable efforts to maintain the integrity of data on the Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents."

J. Other Available Device Information

MAC Address: A Media Access Control address (MAC address), is a unique identifier assigned to network interfaces for communications on the physical network segment. Any Apple product with network interfaces will have one or more MAC addresses, such as Bluetooth, Ethernet, Wi-Fi, or

---

[3] Note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. iOS extractions for serial numbers with either the letter "O" or "I" can not be performed.

[4] The IMEI number is engraved on the back of cellular iPads, the original iPhone, iPhone 5, 5c, 5s, 6, and 6 Plus. For more information, see http://support.apple.com/kb/ht4061. Note that for models with IMEI numbers engraved on the SIM tray, the SIM tray in the device may not be the matching original that came with the device.

FireWire. By providing Apple with a serial number (or in the case of an iOS device, IMEI, MEID, or UDID), this information may be obtained with a subpoena or greater legal process.

UDID: The unique device identifier (UDID) is a sequence of 40 letters and numbers that is specific to a particular iOS device. It will look similar to following: 2j6f0ec908d137be2e1730235f5664094b831186.

If law enforcement is in possession of the device, the device may be connected to iTunes in order to obtain the UDID. Under the iTunes summary tab, the UDID can be revealed by clicking on the serial number.

K. Requests for Apple Retail Store Surveillance Videos

Video surveillance records may vary by store location. Video surveillance records are typically maintained at an Apple store for approximately thirty days. After thirty days, video surveillance may no longer be available. A request for video surveillance can be made at any local Apple retail store. Law enforcement should provide specific date, time, and related transaction information regarding the video requested.

L. Game Center

Game Center is Apple's social gaming network. Information regarding Game Center connections for a user or a device may be available. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Game Center transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific game(s) played.

M. iOS Device Activation

When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available. This information can be obtained with a subpoena or greater legal process.

N. Sign-on Logs

Sign-on activity for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Sign-on transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

O. My Apple ID and iForgot Logs

My Apple ID and iForgot logs for a user may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

P. FaceTime

FaceTime communications are end-to-end encrypted and Apple has no way to decrypt FaceTime data when it is in transit between devices. Apple cannot intercept FaceTime communications. Apple has FaceTime call invitation logs when a FaceTime call invitation is initiated. These logs do not indicate that any communication between users actually took place. Apple has no information as to whether the FaceTime call was successfully established or duration of a FaceTime call. FaceTime call invitation logs are retained up to 30 days. FaceTime call invitation logs can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

IV. Frequently Asked Questions

Can I email Apple with questions regarding my legal process?

Yes, questions or inquiries regarding government legal process can be emailed to subpoenas@apple.com.

I need to personally serve Apple, where should I go?

All personal service can be made at Apple's Cupertino, California headquarters located at the following address:

Apple Inc.
1 Infinite Loop
Cupertino, CA 95014-2084

Can I serve a deposition subpoena directly on an Apple retail store?

No, all subpoenas for testimony, including subpoenas for deposition or trial testimony, need to be personally served on Apple.

I requested information in the body of my email, why was it not provided?

Requests for information not included within the body of the signed subpoena, search warrant, or court order will be disregarded; all information requested must be in the actual executed legal process document.

Can Apple provide me with the passcode of an iOS device that is currently locked?

No, Apple does not have access to a user's passcode but, depending on the version of iOS that the device is running, may be able to extract some data from a passcode locked iOS device running iOS 4 through iOS 7 with a valid search warrant as described in the Guidelines.

Does a device have to be registered with Apple in order to function?

No, a device does not have to be registered with Apple in order for it to function or be used.

Can you help me return a stolen or lost device to the rightful owner?

In cases where law enforcement has recovered a lost or stolen device and wants to return it to the "original owner," contact Apple Customer Care (ACC) via email at law_enforcement_esc@apple.com. Please include the device's serial number in your email and any additional pertinent information. If registration information is available, ACC will contact the owner and instruct him or her to contact law enforcement to recover the device. A subpoena is not required in most cases. However, if there is conflicting information located within our databases you may be instructed to submit a subpoena.

How will the information requested be delivered?

Responsive production of records and information will be sent in an encrypted electronic container via email or, in some instances, via FedEx delivery. If no responsive information is available, a letter indicating this will be sent via email or, in some cases, via U.S. mail.

I am looking into whether a user's email reach the requirements for interstate commerce. Where are the iCloud email servers located?

Apple's U.S. email servers are located in California, Nevada, North Carolina, and Oregon.

Does Apple store GPS information that can be produced under proper legal process?

No, Apple does not track geolocation of devices.

What should be done with the produced files and records when law enforcement has concluded the investigation/criminal case?

Apple requires that any information and data provided to law enforcement containing personally identifiable information (including any copies made) must be destroyed after the related investigation, criminal case, and all appeals have been fully exhausted.

Do you notify users of criminal legal process?

Yes, Apple's notice policy applies to account requests from law enforcement. Apple will notify customers and account holders unless there is a non-disclosure order or applicable law prohibiting notice, or we believe in our sole discretion that such notice may pose immediate risk of serious injury or death to a member of the public, the case relates to a child endangerment matter, or where notice is not applicable to the underlying facts of the case.

Can Apple intercept users' communications pursuant to a Wiretap Order?

Apple can intercept users' email communications, upon receipt of a valid Wiretap Order. Apple cannot intercept users' iMessage or FaceTime communications as these communications are end-to-end encrypted.

V. Appendix A

As per section II (D) above, to request that Apple voluntarily disclose information on an emergency basis, please fill out the Emergency Law Enforcement Information Request form and submit it via email to exigent@apple.com with "Emergency Law Enforcement Information Request" included in the email subject.

The EMERGENCY Law Enforcement Information Request form is available as an editable PDF at: http://www.apple.com/legal/privacy/le-emergencyrequest.pdf

EXHIBIT E

ENGLISH

IMPORTANT: BY USING YOUR iPHONE, iPAD or iPOD TOUCH (“iOS DEVICE”), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS:

A. APPLE iOS SOFTWARE LICENSE AGREEMENT
B. NOTICES FROM APPLE

APPLE INC.
iOS SOFTWARE LICENSE AGREEMENT
Single Use License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR iOS DEVICE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR iOS DEVICE OR DOWNLOADING A SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE iOS DEVICE OR DOWNLOAD THE SOFTWARE UPDATE.

IF YOU HAVE RECENTLY PURCHASED AN iOS DEVICE AND YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE iOS DEVICE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT http://www.apple.com/legal/sales_policies/.

1. General.
(a) The software (including Boot ROM code and other embedded software), documentation, interfaces, content, fonts and any data that came with your iOS Device ("Original iOS Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("iOS Software Updates"), whether in read only memory, on any other media or in any other form (the Original iOS Software and iOS Software Updates are collectively referred to as the “iOS Software") are licensed, not sold, to you by Apple Inc. ("Apple") for use only under the terms of this License. Apple and its licensors retain ownership of the iOS Software itself and reserve all rights not expressly granted to you.

(b) Apple, at its discretion, may make available future iOS Software Updates for your iOS Device. The iOS Software Updates, if any, may not necessarily include all existing software features or new features that Apple releases for newer or other models of iOS Devices. The terms of this License will govern any iOS Software Updates provided by Apple that replace and/or supplement the Original iOS Software product, unless such iOS Software Update is accompanied by a separate license in which case the terms of that license will govern.

2. Permitted License Uses and Restrictions.
(a) Subject to the terms and conditions of this License, you are granted a limited non-exclusive license to use the iOS Software on a single Apple-branded iOS Device. Except as permitted in Section 2(b) below, and unless as provided in a separate agreement between you and Apple, this License does not allow the iOS Software to exist on more than one Apple-branded iOS Device at a time, and you may not distribute or make the iOS Software available over a network where it could be used by multiple devices at the same time. This License does not grant you any rights to use Apple proprietary interfaces and other intellectual property in the design, development, manufacture, licensing or distribution of third party devices and accessories, or third party software applications, for use with iOS Devices. Some of those rights are available under separate licenses from Apple. For more information on developing third party devices and accessories for iOS Devices, please email madeforipod@apple.com. For more information on developing software applications for iOS Devices, please email devprograms@apple.com.

(b) Subject to the terms and conditions of this License, you are granted a limited non-exclusive license to

download iOS Software Updates that may be made available by Apple for your model of the iOS Device to update or restore the software on any such iOS Device that you own or control. This License does not allow you to update or restore any iOS Device that you do not control or own, and you may not distribute or make the iOS Software Updates available over a network where they could be used by multiple devices or multiple computers at the same time. If you download an iOS Software Update to your computer, you may make one copy of the iOS Software Updates stored on your computer in machine-readable form for backup purposes only, provided that the backup copy must include all copyright or other proprietary notices contained on the original.

(c) You may not, and you agree not to or enable others to, copy (except as expressly permitted by this License), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of the iOS Software or any services provided by the iOS Software or any part thereof (except as and only to the extent any foregoing restriction is prohibited by applicable law or by licensing terms governing use of open-source components that may be included with the iOS Software).

(d) By storing content on your iOS Device you are making a digital copy. In some jurisdictions, it is unlawful to make digital copies without prior permission from the rights holder. The iOS Software may be used to reproduce materials so long as such use is limited to reproduction of non-copyrighted materials, materials in which you own the copyright, or materials you are authorized or legally permitted to reproduce.

(e) You agree to use the iOS Software and the Services (as defined in Section 5 below) in compliance with all applicable laws, including local laws of the country or region in which you reside or in which you download or use the iOS Software and Services.

(f) Use of and access to certain features of the iOS Software and certain Services (as defined in Section 5) may require you to apply for a unique user name and password combination, known as an Apple ID. In addition, you acknowledge that many features and Services of the iOS Software transmit data and could impact charges to your data plan, and that you are responsible for any such charges. You can control which applications are permitted to use cellular data and view an estimate of how much data such applications have consumed under Cellular Data Settings. For more information, please consult the User Guide for your iOS Device.

3. Transfer. You may not rent, lease, lend, sell, redistribute, or sublicense the iOS Software. You may, however, make a one-time permanent transfer of all of your license rights to the iOS Software to another party in connection with the transfer of ownership of your iOS Device, provided that: (a) the transfer must include your iOS Device and all of the iOS Software, including all its component parts, original media, printed materials and this License; (b) you do not retain any copies of the iOS Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the iOS Software reads and agrees to accept the terms and conditions of this License.

4. Consent to Use of Data.
(a) Diagnostic and Usage Data. If you opt in to diagnostic and usage collection, you agree that Apple and its subsidiaries and agents may collect, maintain, process and use diagnostic, technical, usage and related information, including but not limited to unique system or hardware identifiers, information about your iOS Device, computer, system and application software, and peripherals, that is gathered periodically to provide and improve Apple's products and services, facilitate the provision of software updates, product support and other services to you (if any) related to the iOS Software, and to verify compliance with the terms of this License. Apple may use this information, as long as it is collected in a form that does not personally identify you, for the purposes described above. If you have opted in and have Location Services turned on, the location of your device may also be sent to help Apple analyze wireless or cellular performance issues (e.g. the strength or weakness of a cellular signal in a particular location). To enable Apple's partners and third party developers to improve their software, hardware and services designed for use with Apple products, Apple may also provide any such partner or third party

developer with a subset of diagnostic information that is relevant to that partner's or developer's software, hardware and/or services, as long as the diagnostic information is in a form that does not personally identify you.

(b) Location Data. Apple and its partners, licensees and third party developers may provide certain services through your iOS Device that rely upon location information. To provide and improve these services, where available, Apple and its partners, licensees and third party developers may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iOS Device, road travel speed information, location search queries, and location of where you purchase and launch applications. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners, licensees and third party developers to provide and improve location-based products and services. **By using any location-based services on your iOS Device, you agree and consent to Apple's and its partners', licensees' and third party developers' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** You may withdraw this consent at any time by going to the Location Services setting on your iOS Device and either turning off the global Location Services setting or turning off the individual location settings of each location-aware item on your iOS Device. When using third party applications or services on the iOS Device that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services.

(c) Siri and Dictation. The Siri and Dictation features of the iOS Software may not be available in all languages or regions and features may vary by region. If your iOS Device supports Siri and Dictation, these features may allow you to make requests, give commands and dictate text to your device using your voice. When you use Siri or Dictation, the things you say will be recorded and sent to Apple in order to convert what you say into text and to process your requests. Your device will also send Apple other information, such as your name and nickname; the names, nicknames, and relationship with you (e.g., "my dad") of your address book contacts; and song names in your collection (collectively, your "User Data"). All of this data is used to help Siri and Dictation understand you better and recognize what you say. It is not linked to other data that Apple may have from your use of other Apple services. **By using Siri or Dictation, you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this information, including your voice input and User Data, to provide and improve Siri, Dictation, and dictation functionality in other Apple products and services.**

If you have Location Services turned on, the location of your iOS Device at the time you make a request to Siri may also be sent to Apple to help Siri improve the accuracy of its response to your location-based requests. You may disable the location-based functionality of Siri by going to the Location Services setting on your iOS Device and turning off the individual location setting for Siri.

Siri can allow you to interact with your iOS Device without needing to unlock it. If you have enabled a passcode on your iOS Device and would like to prevent Siri from being used from the lock screen, you can tap Settings, tap General, tap Passcode Lock and turn the Siri option to "off".

You can also turn off Siri and Dictation altogether at any time. To do so, open Settings, tap General, tap Siri, and slide the Siri switch to "off".

(d) FaceTime. The FaceTime calling feature of the iOS Software ("FaceTime") requires a Wi-Fi or cellular data connection and may not be available in all regions and may be restricted or unavailable from your service provider. Your use of FaceTime is subject to your compliance with Section 2(e) above. In order to set up FaceTime, and to initiate and receive FaceTime calls between you and other FaceTime users, certain unique identifiers for your iOS Device and account are needed. These unique identifiers may include your email address(es), the Apple ID information you provide, a hardware identifier for your iOS Device, and your iPhone's telephone number. **By using the iOS Software, you agree that Apple may transmit, collect, maintain, process and use these identifiers for the purpose of providing and**

improving the FaceTime feature. You understand that your iPhone's telephone number will be displayed to the other party on the call (even if you have a blocked number) or your email address will be shown, depending on what setting you choose. You may turn off the FaceTime feature by going to the FaceTime setting on your iOS Device or by going to the Restrictions setting and enabling the FaceTime restriction. You may also restrict FaceTime to Wi-Fi only, by going to the FaceTime setting on your iOS Device and sliding the "Use Cellular Data" switch to "Off".

(e) iMessage. The messaging feature of the iOS Software ("iMessage") may not be available in all countries or regions. Your use of iMessage is subject to your compliance with Section 2(e) above. In order to set up iMessage, and to initiate and receive iMessages between you and other iOS Device users, certain unique identifiers for your iOS Device and account are needed. These unique identifiers may include your email address(es), the Apple ID information you provide, a hardware identifier for your iOS Device, and your iPhone's telephone number. **By using the iOS Software, you agree that Apple may transmit, collect, maintain, process and use these identifiers for the purpose of providing and improving the iMessage service.** The iMessage service requires a Wi-Fi or cellular data connection. To facilitate delivery of your iMessages and to enable you to maintain conversations across your devices, Apple may hold your iMessages in encrypted form for a limited period of time. If your message cannot be sent as an iMessage, your message may be sent as an SMS or MMS message, for which carrier messaging rates may apply. You understand that your iPhone's telephone number will be displayed to the other party (even if you have a blocked number) or your email address will be shown, depending on what setting you choose. You may turn off the iMessage service by going to the Messages setting on your iOS Device.

(f) My Photo Stream. **By using the My Photo Stream feature of iCloud, you agree that Apple may store photos taken on your iOS Device or uploaded from your computer for a limited period of time and automatically send the photos to your other Apple iOS Devices or computers that have My Photo Stream enabled.** Please note that a limited number of photos may be stored in the cloud or on your devices at any one time, and older photos will be automatically deleted from My Photo Stream over time. Any photos you want to keep on a particular device permanently must be saved to the camera roll or the photo library on your computer. Photo resolution may vary depending on the device to which the photos are downloaded. If you do not wish to use My Photo Stream, you can turn My Photo Stream off on all of your iOS Devices or computers that have My Photo Stream enabled. All use of the My Photo Stream feature is subject to the terms and conditions of this agreement and the iCloud Terms and Conditions located at: http://www.apple.com/legal/icloud/ww/.

(g) iCloud Photo Sharing. **By using the iCloud Photo Sharing feature, you agree that Apple may store the photos and videos you share continuously until you delete them, send those photos and videos to your other Apple iOS devices and computers that have iCloud Photo Sharing enabled, and send them to the iOS devices and computers of the people you choose to share them with.** When you use iCloud Photo Sharing, you are allowing your recipients to view, save, copy, and share your photos and videos, as well as contribute photos and videos, and leave comments. You can delete individual photos, videos, comments, or entire shared photo streams at any time to stop sharing them immediately, however, photos and videos that the viewer has previously saved to their device or computer will not be deleted. All use of the iCloud Photo Sharing feature is subject to the terms and conditions of this agreement and the iCloud Terms and Conditions located at: http://www.apple.com/legal/icloud/ww/.

(h) Maps. The maps service and features of the iOS Software ("Maps") may not be available in all languages or regions, and features and map data coverage may vary by region. Use of the Maps service requires a Wi-Fi or cellular data connection. When you use any location-based features within Maps, such as turn-by-turn navigation, traffic and local search, various location-related and usage information may be sent to Apple, including the real-time geographic location of your iOS Device, in order to process your request and help improve Maps. Such location and usage data is collected by Apple in a form that does not personally identify you. **By using Maps, you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this**

information, to provide and improve the Maps features and service, and other Apple products and services.

If you have Location Services turned on, the location of your iOS Device at the time you make a request to Maps may also be sent to Apple if required to process the request, such as turn-by-turn navigation. You may disable the location-based functionality of Maps by going to the Location Services setting on your iOS Device and turning off the individual location setting for Maps. Certain Maps features will however be unavailable if you disable the Location Services setting, such as turn-by-turn navigation.

(i) Interest-Based Advertising from iAd. Apple may provide mobile, interest-based advertising to you. If you do not want to receive relevant ads on your iOS Device, you can opt out by going to the Limit Ad Tracking setting on your iOS Device. If you opt out, you will continue to receive the same number of mobile ads, but they may be less relevant because they will not be based on your interests. You may still see ads related to the content on a web page or in an application or based on other non-personal information.

(j) Privacy Policy. At all times your information will be treated in accordance with Apple's Privacy Policy, which is incorporated by reference into this License and can be viewed at: http://www.apple.com/privacy/.

5. Services and Third Party Materials.
(a) The iOS Software may enable access to Apple's iTunes Store, App Store, Game Center, iCloud, Maps and other Apple and third party services and web sites (collectively and individually, "Services"). Such Services may not be available in all languages or in all countries. Use of these Services requires Internet access and use of certain Services may require an Apple ID, may require you to accept additional terms and may be subject to additional fees. By using this software in connection with an Apple ID, or other Apple Service, you agree to the applicable terms of service for that Service, such as the latest iTunes Store Terms and Conditions or Game Center Terms and Conditions, which you may access and review at http://www.apple.com/legal/itunes/ww/, or the iCloud Terms and Conditions which can be found at http://www.apple.com/legal/icloud/ww/, respectively.

(b) If you sign up for iCloud, certain iCloud features like "Back Up" and "Find My iPhone" may be accessed directly from the iOS Software. You acknowledge and agree that your use of iCloud and these features is subject to the latest terms and conditions of the iCloud service, which you may access and review at: http://www.apple.com/legal/icloud/ww/.

(c) You understand that by using any of the Services, you may encounter content that may be deemed offensive, indecent, or objectionable, which content may or may not be identified as having explicit language, and that the results of any search or entering of a particular URL may automatically and unintentionally generate links or references to objectionable material. Nevertheless, you agree to use the Services at your sole risk and that Apple shall have no liability to you for content that may be found to be offensive, indecent, or objectionable.

(d) Certain Services may display, include or make available content, data, information, applications or materials from third parties ("Third Party Materials") or provide links to certain third party web sites. By using the Services, you acknowledge and agree that Apple is not responsible for examining or evaluating the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect of such Third Party Materials or web sites. Apple, its officers, affiliates and subsidiaries do not warrant or endorse and do not assume and will not have any liability or responsibility to you or any other person for any third-party Services, Third Party Materials or web sites, or for any other materials, products, or services of third parties. Third Party Materials and links to other web sites are provided solely as a convenience to you.

(e) Neither Apple nor any of its content providers guarantees the availability, accuracy, completeness, reliability, or timeliness of stock information, location data or any other data displayed by any Services.

Financial information displayed by any Services is for general informational purposes only and should not be relied upon as investment advice. Before executing any securities transaction based upon information obtained through the Services, you should consult with a financial or securities professional who is legally qualified to give financial or securities advice in your country or region. Location data provided by any Services, including the Apple Maps service, is provided for basic navigational and/or planning purposes only and is not intended to be relied upon in situations where precise location information is needed or where erroneous, inaccurate, time-delayed or incomplete location data may lead to death, personal injury, property or environmental damage. You agree that, the results you receive from the Maps service may vary from actual road or terrain conditions due to factors that can affect the accuracy of the Maps data, such as, but not limited to, weather, road and traffic conditions, and geopolitical events. For your safety when using the navigation feature, always pay attention to posted road signs and current road conditions. Follow safe driving practices and traffic regulations, and note that walking directions may not include sidewalks or pedestrian paths.

(f) To the extent that you upload any content through the use of the Services, you represent that you own all rights in, or have authorization or are otherwise legally permitted to upload, such content and that such content does not violate any terms of service applicable to the Services. You agree that the Services contain proprietary content, information and material that is owned by Apple, the site owner and/or their licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright. You agree that you will not use such proprietary content, information or materials other than for permitted use of the Services or in any manner that is inconsistent with the terms of this License or that infringes any intellectual property rights of a third party or Apple. No portion of the Services may be reproduced in any form or by any means. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the Services, in any manner, and you shall not exploit the Services in any unauthorized way whatsoever, including but not limited to, using the Services to transmit any computer viruses, worms, trojan horses or other malware, or by trespass or burdening network capacity. You further agree not to use the Services in any manner to harass, abuse, stalk, threaten, defame or otherwise infringe or violate the rights of any other party, and that Apple is not in any way responsible for any such use by you, nor for any harassing, threatening, defamatory, offensive, infringing or illegal messages or transmissions that you may receive as a result of using any of the Services.

(g) In addition, Services and Third Party Materials that may be accessed, linked to or displayed on the iOS Device are not available in all languages or in all countries or regions. Apple makes no representation that such Services and Third Party Materials are appropriate or available for use in any particular location. To the extent you choose to use or access such Services and Third Party Materials, you do so at your own initiative and are responsible for compliance with any applicable laws, including but not limited to applicable local laws and privacy and data collection laws. Apple and its licensors reserve the right to change, suspend, remove, or disable access to any Services at any time without notice. In no event will Apple be liable for the removal of or disabling of access to any such Services. Apple may also impose limits on the use of or access to certain Services, in any case and without notice or liability.

6. Termination. This License is effective until terminated. Your rights under this License will terminate automatically or otherwise cease to be effective without notice from Apple if you fail to comply with any term(s) of this License. Upon the termination of this License, you shall cease all use of the iOS Software. Sections 4, 5, 6, 7, 8, 9, 12 and 13 of this License shall survive any such termination.

7. Disclaimer of Warranties.

7.1 If you are a customer who is a consumer (someone who uses the iOS Software outside of your trade, business or profession), you may have legal rights in your country of residence which would prohibit the following limitations from applying to you, and where prohibited they will not apply to you. To find out more about rights, you should contact a local consumer advice organization.

7.2 YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT, TO THE EXTENT PERMITTED BY

APPLICABLE LAW, USE OF THE iOS SOFTWARE AND ANY SERVICES PERFORMED BY OR ACCESSED THROUGH THE iOS SOFTWARE IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU.

7.3 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE iOS SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND APPLE AND APPLE'S LICENSORS (COLLECTIVELY REFERRED TO AS "APPLE" FOR THE PURPOSES OF SECTIONS 7 AND 8) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE iOS SOFTWARE AND SERVICES, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

7.4 APPLE DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE iOS SOFTWARE AND SERVICES, THAT THE FUNCTIONS CONTAINED IN, OR SERVICES PERFORMED OR PROVIDED BY, THE iOS SOFTWARE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE iOS SOFTWARE AND SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, THAT ANY SERVICE WILL CONTINUE TO BE MADE AVAILABLE, THAT DEFECTS IN THE iOS SOFTWARE OR SERVICES WILL BE CORRECTED, OR THAT THE iOS SOFTWARE WILL BE COMPATIBLE OR WORK WITH ANY THIRD PARTY SOFTWARE, APPLICATIONS OR THIRD PARTY SERVICES. INSTALLATION OF THIS iOS SOFTWARE MAY AFFECT THE USABILITY OF THIRD PARTY SOFTWARE, APPLICATIONS OR THIRD PARTY SERVICES.

7.5 YOU FURTHER ACKNOWLEDGE THAT THE iOS SOFTWARE AND SERVICES ARE NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN, THE CONTENT, DATA OR INFORMATION PROVIDED BY THE iOS SOFTWARE OR SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE, INCLUDING WITHOUT LIMITATION THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT OR WEAPONS SYSTEMS.

7.6 NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY APPLE OR AN APPLE AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE iOS SOFTWARE OR SERVICES PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

8. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL APPLE BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, CORRUPTION OR LOSS OF DATA, FAILURE TO TRANSMIT OR RECEIVE ANY DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE iOS SOFTWARE AND SERVICES OR ANY THIRD PARTY SOFTWARE OR APPLICATIONS IN CONJUNCTION WITH THE iOS SOFTWARE OR SERVICES, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Apple's total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of two hundred and fifty dollars (U.S.$250.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

9. Digital Certificates. The iOS Software contains functionality that allows it to accept digital certificates

either issued from Apple or from third parties. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON A CERTIFICATE WHETHER ISSUED BY APPLE OR A THIRD PARTY. YOUR USE OF DIGITAL CERTIFICATES IS AT YOUR SOLE RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, APPLE MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ACCURACY, SECURITY, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH RESPECT TO DIGITAL CERTIFICATES.

10. Export Control. You may not use or otherwise export or re-export the iOS Software except as authorized by United States law and the laws of the jurisdiction(s) in which the iOS Software was obtained. In particular, but without limitation, the iOS Software may not be exported or re-exported (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List. By using the iOS Software, you represent and warrant that you are not located in any such country or on any such list. You also agree that you will not use the iOS Software for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of missiles, nuclear, chemical or biological weapons.

11. Government End Users. The iOS Software and related documentation are "Commercial Items", as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

12. Controlling Law and Severability. This License will be governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles. This License shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If you are a consumer based in the United Kingdom, this License will be governed by the laws of the jurisdiction of your residence. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.

13. Complete Agreement; Governing Language. This License constitutes the entire agreement between you and Apple relating to the iOS Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by Apple. Any translation of this License is done for local requirements and in the event of a dispute between the English and any non-English versions, the English version of this License shall govern, to the extent not prohibited by local law in your jurisdiction.

14. Third Party Acknowledgements. Portions of the iOS Software may utilize or include third party software and other copyrighted material. Acknowledgements, licensing terms and disclaimers for such material are contained in the electronic documentation for the iOS Software, and your use of such material is governed by their respective terms. Use of the Google Safe Browsing Service is subject to the Google Terms of Service (http://www.google.com/terms_of_service.html) and to Google's Privacy Policy (http://www.google.com/privacypolicy.html).

15. Use of MPEG-4; H.264/AVC Notice.
(a) The iOS Software contains MPEG-4 video encoding and/or decoding functionality. The iOS Software is licensed under the MPEG-4 Visual Patent Portfolio License for the personal and non-commercial use of a consumer for (i) encoding video in compliance with the MPEG-4 Visual Standard ("MPEG-4 Video") and/or (ii) decoding MPEG-4 video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed by MPEG LA to provide MPEG-4

video. No license is granted or shall be implied for any other use. Additional information including that relating to promotional, internal and commercial uses and licensing may be obtained from MPEG LA, LLC. See http://www.mpegla.com.

(b) The iOS Software contains AVC encoding and/or decoding functionality, commercial use of H.264/ AVC requires additional licensing and the following provision applies: THE AVC FUNCTIONALITY IN THE iOS SOFTWARE IS LICENSED HEREIN ONLY FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR AVC VIDEO THAT WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. INFORMATION REGARDING OTHER USES AND LICENSES MAY BE OBTAINED FROM MPEG LA L.L.C. SEE HTTP://WWW.MPEGLA.COM.

16. Yahoo Search Service Restrictions. The Yahoo Search Service available through Safari is licensed for use only in the following countries and regions: Argentina, Aruba, Australia, Austria, Barbados, Belgium, Bermuda, Brazil, Bulgaria, Canada, Cayman Islands, Chile, China, Colombia, Cyprus, Czech Republic, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, France, Germany, Greece, Grenada, Guatemala, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Jamaica, Japan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, New Zealand, Nicaragua, Norway, Panama, Peru, Philippines, Poland, Portugal, Puerto Rico, Romania, Singapore, Slovakia, Slovenia, South Korea, Spain, St. Lucia, St. Vincent, Sweden, Switzerland, Taiwan, Thailand, The Bahamas, Trinidad and Tobago, Turkey, UK, Uruguay, US and Venezuela.

17. Microsoft Exchange Notice. The Microsoft Exchange mail setting in the iOS Software is licensed only for over-the-air synchronization of information, such as email, contacts, calendar and tasks, between your iOS and Microsoft Exchange Server or other server software licensed by Microsoft to implement the Microsoft Exchange ActiveSync protocol.

EA1040
7/24/2013

NOTICES FROM APPLE

If Apple needs to contact you about your product or account, you consent to receive the notices by email. You agree that any such notices that we send you electronically will satisfy any legal communication requirements.

FRANÇAIS

IMPORTANT : L'UTILISATION DE VOTRE iPHONE, iPAD ou IPOD TOUCH (« APPAREIL iOS ») IMPLIQUE QUE VOUS ACCEPTEZ D'ÊTRE LIÉ PAR LES CONDITIONS SUIVANTES :

A. CONTRAT DE LICENCE DE LOGICIEL DE L'APPLE iOS
B. NOTIFICATIONS DE LA PART D'APPLE

APPLE INC.
CONTRAT DE LICENCE DE LOGICIEL DE L'APPLE iOS
Licence individuelle

LISEZ ATTENTIVEMENT CE CONTRAT DE LICENCE DE LOGICIEL (LA « LICENCE ») AVANT D'UTILISER VOTRE APPAREIL iOS OU DE TÉLÉCHARGER LA MISE À JOUR DU LOGICIEL FOURNI AVEC LA PRÉSENTE LICENCE. L'UTILISATION DE VOTRE APPAREIL iOS OU LE TÉLÉCHARGEMENT D'UNE MISE À JOUR, LE CAS ÉCHÉANT, IMPLIQUE QUE VOUS ACCEPTEZ LES CONDITIONS DE CETTE LICENCE. SI VOUS ÊTES EN DÉSACCORD AVEC LES CONDITIONS DE CETTE LICENCE, N'UTILISEZ PAS L'APPAREIL iOS ET NE TÉLÉCHARGEZ PAS CETTE MISE À

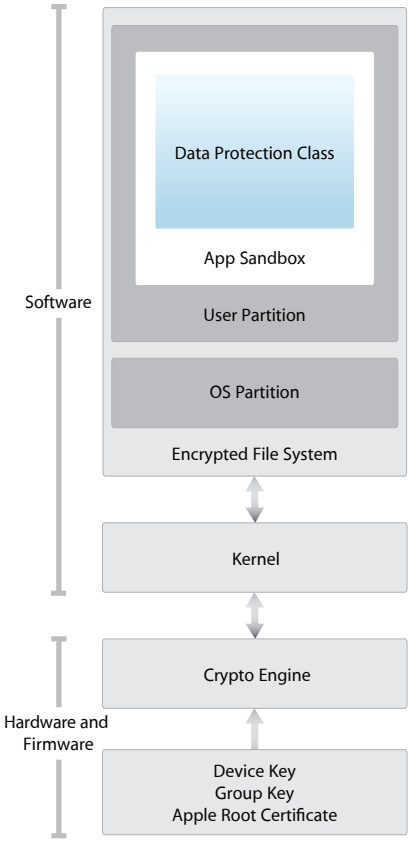
EXHIBIT F

iOS Security

February 2014

Contents

Introduction



Security architecture diagram of iOS provides a visual overview of the different technologies discussed in this document.

Apple designed the iOS platform with security at its core. When we set out to create the best possible mobile OS, we drew from decades of experience to build an entirely new architecture. We thought about the security hazards of the desktop environment, and established a new approach to security in the design of iOS. We developed and incorporated innovative features that tighten mobile security and protect the entire system by default. As a result, iOS is a major leap forward in OS security.

Every iOS device combines software, hardware, and services designed to work together for maximum security and a transparent user experience. iOS protects not only the device and its data at rest, but the entire ecosystem, including everything users do locally, on networks, and with key Internet services.

iOS and iOS devices provide stringent security features, and they're easy to use. Many of these features are enabled by default, so IT departments don't need to perform extensive configurations. And key security features like device encryption are not configurable, so users can't disable them by mistake. Other features, such as Touch ID, enhance the user experience by making it simpler and more intuitive to secure the device.

This document provides details about how security technology and features are implemented within the iOS platform. It will also help organizations combine iOS platform security technology and features with their own policies and procedures to meet their specific security needs.

- **System security:** The integrated and secure software and hardware that are the platform for iPhone, iPad, and iPod touch.
- **Encryption and data protection:** The architecture and design that protect user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it.
- **App security:** The systems that enable apps to run securely and without compromising platform integrity.
- **Network security:** Industry-standard networking protocols that provide secure authentication and encryption of data in transmission.
- **Internet services:** Apple's network-based infrastructure for messaging, syncing, and backup.
- **Device controls:** Methods that prevent unauthorized use of the device and enable it to be remotely wiped if lost or stolen.

System Security

System security is designed so that both software and hardware are secure across all core components of every iOS device. This includes the boot-up process, software updates, and secure enclave. This architecture is central to security in iOS, and never gets in the way of device usability.

The tight integration of hardware and software on iOS devices ensures that each component of the system is trusted, and validates the system as a whole. From initial boot-up to iOS software updates to third-party apps, each step is analyzed and vetted to help ensure that the hardware and software are performing optimally together and using resources properly.

Secure Boot Chain

Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware.

When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.

This secure boot chain helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices.

For devices with cellular access, the baseband subsystem also utilizes its own similar process of secure booting with signed software and keys verified with the broadband subsystem.

For devices with an A7 processor, the Secure Enclave coprocessor also utilizes a secure boot process that ensures its separate software is verified and signed by Apple.

If one step of this boot process is unable to load or verify the next process, startup is stopped and the device displays the "Connect to iTunes" screen. This is called recovery mode. If the Boot ROM is not even able to load or verify LLB, it enters DFU (Device Firmware Upgrade) mode. In both cases, the device must be connected to iTunes via USB and restored to factory default settings. For more information on manually entering recovery mode, see http://support.apple.com/kb/HT1808.

Entering Device Firmware Upgrade (DFU) mode
Restoring a device after it enters DFU mode returns it to a known good state with the certainty that only unmodified Apple-signed code is present. DFU mode can be entered manually: First connect the device to a computer using a USB cable, then hold down both the Home and Sleep/Wake buttons. After 8 seconds, release the Sleep/Wake button while continuing to hold down the Home button. Note: Nothing will be displayed on the screen when it's in DFU mode. If the Apple logo appears, the Sleep/Wake button was held down too long.

System Software Authorization

Apple regularly releases software updates to address emerging security concerns and also provide new features; these updates are typically provided for all supported devices simultaneously. Users receive iOS update notifications on the device and through iTunes, and updates are delivered wirelessly, encouraging rapid adoption of the latest security fixes.

The startup process described above helps ensure that only Apple-signed code can be installed on a device. To prevent devices from being downgraded to older versions that lack the latest security updates, iOS uses a process called System Software Authorization. If downgrades were possible, an attacker who gains possession of a device could install an older version of iOS and exploit a vulnerability that's been fixed in the newer version.

On a device with an A7 processor, the Secure Enclave coprocessor also utilizes System Software Authorization to ensure the integrity of its software and prevent downgrade installations. See "Secure Enclave," below.

iOS software updates can be installed using iTunes or over the air (OTA) on the device. With iTunes, a full copy of iOS is downloaded and installed. OTA software updates download only the components required to complete an update, improving network efficiency rather than downloading the entire OS. Additionally, software updates can be cached on a local network server running OS X Server so that iOS devices do not need to access Apple servers to obtain the necessary update data.

During an iOS upgrade, iTunes (or the device itself, in the case of OTA software updates) connects to the Apple installation authorization server and sends it a list of cryptographic measurements for each part of the installation bundle to be installed (for example, LLB, iBoot, the kernel, and OS image), a random anti-replay value (nonce), and the device's unique ID (ECID).

The authorization server checks the presented list of measurements against versions for which installation is permitted, and if it finds a match, adds the ECID to the measurement and signs the result. The server passes a complete set of signed data to the device as part of the upgrade process. Adding the ECID "personalizes" the authorization for the requesting device. By authorizing and signing only for known measurements, the server ensures that the update takes place exactly as provided by Apple.

The boot-time chain-of-trust evaluation verifies that the signature comes from Apple and that the measurement of the item loaded from disk, combined with the device's ECID, matches what was covered by the signature.

These steps ensure that the authorization is for a specific device and that an old iOS version from one device can't be copied to another. The nonce prevents an attacker from saving the server's response and using it to tamper with a device or otherwise alter the system software.

Secure Enclave

The Secure Enclave is a coprocessor fabricated in the Apple A7 chip. It utilizes its own secure boot and personalized software update separate from the application processor. It also provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised.

The Secure Enclave uses encrypted memory and includes a hardware random number generator. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

Each Secure Enclave is provisioned during fabrication with its own UID (Unique ID) that is not accessible to other parts of the system and is not known to Apple. When the device starts up, an ephemeral key is created, tangled with its UID, and used to encrypt the Secure Enclave's portion of the device's memory space.

Additionally, data that is saved to the file system by the Secure Enclave is encrypted with a key tangled with the UID and an anti-replay counter.

The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchase on behalf of the user. Communication between the A7 and the Touch ID sensor takes place over a serial peripheral interface bus. The A7 forwards the data to the Secure Enclave but cannot read it. It's encrypted and authenticated with a session key that is negotiated using the device's shared key that is built into the Touch ID sensor and the Secure Enclave. The session key exchange uses AES key wrapping with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption.

Touch ID

Touch ID is the fingerprint sensing system built into iPhone 5s, making secure access to the device faster and easier. This forward-thinking technology reads fingerprints from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use.

Touch ID makes using a longer, more complex passcode far more practical because users won't have to enter it as frequently. Touch ID also overcomes the inconvenience of a passcode-based lock, not by replacing it but rather by securely providing access to the device within thoughtful boundaries and time constraints.

Touch ID and passcodes

To use Touch ID, users must set up iPhone 5s so that it requires a passcode to unlock the device. When Touch ID scans and recognizes an enrolled fingerprint, iPhone 5s unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances:

- iPhone 5s has just been turned on or restarted
- iPhone 5s has not been unlocked for more than 48 hours
- After five unsuccessful attempts to match a finger
- When setting up or enrolling new fingers with Touch ID
- iPhone 5s has received a remote lock command

When Touch ID is enabled, iPhone immediately locks when the Sleep/Wake button is pressed. With passcode-only security, many users set an unlocking grace period to avoid having to enter a passcode each time the device is used. With Touch ID, iPhone 5s locks every time it goes to sleep, and requires a fingerprint—or optionally the passcode—at every wake.

Touch ID can be trained to recognize up to five different fingers. With one finger enrolled, the chance of a random match with someone else is 1 in 50,000. However, Touch ID allows only five unsuccessful fingerprint match attempts before the user is required to enter a passcode to obtain access.

Other uses for Touch ID

Touch ID can also be configured to approve purchases from the iTunes Store, the App Store, and the iBooks Store, so users don't have to enter an Apple ID password. When users choose to authorize a purchase, authentication tokens are exchanged between the device and store. The token and nonce are held in the Secure Enclave. The nonce is signed with a Secure Enclave key shared by all devices and the iTunes Store.

Touch ID authentication and the data associated with the enrolled fingerprints are not available to other apps or third parties.

Touch ID security

The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave.

The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded after. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes never leaves iPhone 5s, is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes.

How Touch ID unlocks iPhone 5s

On devices with an A7 processor, the Secure Enclave holds the cryptographic class keys for Data Protection. When a device locks, the keys for Data Protection class Complete are discarded, and files and keychain items in that class are inaccessible until the user unlocks the device by entering their passcode.

On iPhone 5s with Touch ID turned on, the keys are not discarded when the device locks; instead, they're wrapped with a key that is given to the Touch ID subsystem. When a user attempts to unlock the device, if Touch ID recognizes the user's fingerprint, it provides the key for unwrapping the Data Protection keys and the device is unlocked. This process provides additional protection by requiring the Data Protection and Touch ID subsystems to cooperate in order to unlock the device.

The decrypted class keys are only held in memory, so they're lost if the device is rebooted. Additionally, as previously described, the Secure Enclave will discard the keys after 48 hours or 5 failed Touch ID recognition attempts.

Encryption and Data Protection

The secure boot chain, code signing, and runtime process security all help to ensure that only trusted code and apps can run on a device. iOS has additional encryption and data protection features to safeguard user data, even in cases where other parts of the security infrastructure have been compromised (for example, on a device with unauthorized modifications). This provides important benefits for both users and IT administrators, protecting personal and corporate information at all times and providing methods for instant and complete remote wipe in the case of device theft or loss.

Hardware Security Features

On mobile devices, speed and power efficiency are critical. Cryptographic operations are complex and can introduce performance or battery life problems if not designed and implemented with these priorities in mind.

Every iOS device has a dedicated AES 256 crypto engine built into the DMA path between the flash storage and main system memory, making file encryption highly efficient. Along with the AES engine, SHA-1 is implemented in hardware, further reducing cryptographic operation overhead.

The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused into the application processor during manufacturing. No software or firmware can read them directly; they can see only the results of encryption or decryption operations performed using them. The UID is unique to each device and is not recorded by Apple or any of its suppliers. The GID is common to all processors in a class of devices (for example, all devices using the Apple A7 chip), and is used as an additional level of protection when delivering system software during installation and restore. Integrating these keys into the silicon helps prevent them from being tampered with or bypassed, or accessed outside the AES engine.

The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if the memory chips are physically moved from one device to another, the files are inaccessible. The UID is not related to any other identifier on the device.

Apart from the UID and GID, all other cryptographic keys are created by the system's random number generator (RNG) using an algorithm based on CTR_DRBG. System entropy is gathered from interrupt timing during boot, and additionally from internal sensors once the device has booted.

Securely erasing saved keys is just as important as generating them. It's especially challenging to do so on flash storage, where wear-leveling might mean multiple copies of data need to be erased. To address this issue, iOS devices include a feature dedicated to secure data erasure called Effaceable Storage. This feature accesses the underlying storage technology (for example, NAND) to directly address and erase a small number of blocks at a very low level.

Erase all content and settings
The "Erase all content and settings" option in Settings obliterates all the keys in Effaceable Storage, rendering all user data on the device cryptographically inaccessible. Therefore, it's an ideal way to be sure all personal information is removed from a device before giving it to somebody else or returning it for service. Important: Do not use the "Erase all content and settings" option until the device has been backed up, as there is no way to recover the erased data.

File Data Protection

In addition to the hardware encryption features built into iOS devices, Apple uses a technology called Data Protection to further protect data stored in flash memory on the device. Data Protection allows the device to respond to common events such as incoming phone calls, but also enables a high level of encryption for sensitive data. Mail uses Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically.

Data Protection is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into each iOS device. Data Protection is controlled on a per-file basis by assigning each file to a class; accessibility is determined by whether the class keys have been unlocked.

Architecture overview

Every time a file on the data partition is created, Data Protection creates a new 256-bit key (the "per-file" key) and gives it to the hardware AES engine, which uses the key to encrypt the file as it is written to flash memory using AES CBC mode. The initialization vector (IV) is the output of a linear feedback shift register (LFSR) calculated with the block offset into the file, encrypted with the SHA-1 hash of the per-file key.

The per-file key is wrapped with one of several class keys, depending on the circumstances under which the file should be accessible. Like all other wrappings, this is performed using NIST AES key wrapping, per RFC 3394. The wrapped per-file key is stored in the file's metadata.

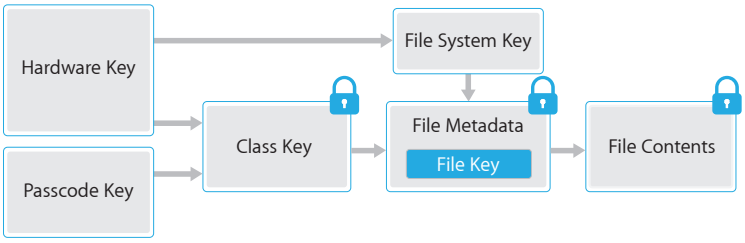
When a file is opened, its metadata is decrypted with the file system key, revealing the wrapped per-file key and a notation on which class protects it. The per-file key is unwrapped with the class key, then supplied to the hardware AES engine, which decrypts the file as it is read from flash memory.

Creating strong Apple ID passwords

Apple IDs are used to connect to a number of services including iCloud, FaceTime, and iMessage. To help users create strong passwords, all new accounts must contain the following password attributes:

- At least eight characters
- At least one letter
- At least one uppercase letter
- At least one number
- No more than three consecutive identical characters
- Not the same as the account name

The metadata of all files in the file system is encrypted with a random key, which is created when iOS is first installed or when the device is wiped by a user. The file system key is stored in Effaceable Storage. Since it's stored on the device, this key is not used to maintain the confidentiality of data; instead, it's designed to be quickly erased on demand (by the user, with the "Erase all content and settings" option, or by a user or administrator issuing a remote wipe command from a mobile device management server, Exchange ActiveSync, or iCloud). Erasing the key in this manner renders all files cryptographically inaccessible.



The content of a file is encrypted with a per-file key, which is wrapped with a class key and stored in a file's metadata, which is in turn encrypted with the file system key. The class key is protected with the hardware UID and, for some classes, the user's passcode. This hierarchy provides both flexibility and performance. For example, changing a file's class only requires rewrapping its per-file key, and a change of passcode just rewraps the class key.

Passcodes

By setting up a device passcode, the user automatically enables Data Protection. iOS supports four-digit and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides the entropy for encryption keys, which are not stored on the device. This means an attacker in possession of a device can't get access to data in certain protection classes without the passcode.

The passcode is "tangled" with the device's UID, so brute-force attempts must be performed on the device under attack. A large iteration count is used to make each attempt slower. The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.

The stronger the user passcode is, the stronger the encryption key becomes. Touch ID on iPhone 5s can be used to enhance this equation by enabling the user to establish a much stronger passcode than would otherwise be practical. This increases the effective amount of entropy protecting the encryption keys used for Data Protection without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day.

Passcode considerations
If a long password that contains only numbers is entered, a numeric keypad is displayed at the Lock screen instead of the full keyboard. A longer numeric passcode may be easier to enter than a shorter alphanumeric passcode, while providing similar security.

To further discourage brute-force passcode attacks, the iOS interface enforces escalating time delays after the entry of an invalid passcode at the Lock screen. Users can choose to have the device automatically wiped if the passcode is entered incorrectly after 10 consecutive attempts. This setting is also available as an administrative policy through mobile device management (MDM) and Exchange ActiveSync, and can also be set to a lower threshold.

On a device with an A7 processor, the key operations are performed by the Secure Enclave, which also enforces a 5-second delay between repeated failed unlocking requests. This provides a governor against brute-force attacks in addition to safeguards enforced by iOS.

Data Protection Classes

When a new file is created on an iOS device, it's assigned a class by the app that creates it. Each class uses different policies to determine when the data is accessible. The basic classes and policies are as follows.

Complete Protection

(`NSFileProtectionComplete`**):** The class key is protected with a key derived from the user passcode and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks the device using Touch ID.

The Mail app implements Complete Protection for messages and attachments. App launch images and location data are also stored with Complete Protection.

Protected Unless Open

(`NSFileProtectionCompleteUnlessOpen`**):** Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background. This behavior is achieved by using asymmetric elliptic curve cryptography (ECDH over Curve25519). Along with the usual per-file key, Data Protection generates a file public/private key pair. A shared secret is computed using the file's private key and the Protected Unless Open class public key, whose corresponding private key is protected with the user's passcode and the device UID. The per-file key

is wrapped with the hash of this shared secret and stored in the file's metadata along with the file's public key; the corresponding private key is then wiped from memory. As soon as the file is closed, the per-file key is also wiped from memory. To open the file again, the shared secret is re-created using the Protected Unless Open class's private key and the file's ephemeral public key; its hash is used to unwrap the per-file key, which is then used to decrypt the file.

Protected Until First User Authentication

(`NSFileProtectionCompleteUntilFirstUserAuthentication`**):** This class behaves in the same way as Complete Protection, except that the decrypted class key is not removed from memory when the device is locked. The protection in this class has similar properties to desktop full-disk encryption, and protects data from attacks that involve a reboot. This is the default class for all third-party app data not otherwise assigned to a Data Protection class.

No Protection

(`NSFileProtectionNone`**):** This class key is protected only with the UID, and is kept in Effaceable Storage. Since all the keys needed to decrypt files in this class are stored on the device, the encryption only affords the benefit of fast remote wipe. If a file is not assigned a Data Protection class, it is still stored in encrypted form (as is all data on an iOS device).

Components of a keychain item

Along with the access group, each keychain item contains administrative metadata (such as "created" and "last updated" time stamps). It also contains SHA-1 hashes of the attributes used to query for the item (such as the account and server name) to allow lookup without decrypting each item. And finally, it contains the encryption data, which includes the following:

- Version number
- Value indicating which protection class the item is in
- Per-item key wrapped with the protection class key
- Dictionary of attributes describing the item (as passed to SecItemAdd), encoded as a binary plist and encrypted with the per-item key

The encryption is AES 128 in GCM (Galois/Counter Mode); the access group is included in the attributes and protected by the GMAC tag calculated during encryption.

Keychain Data Protection

Many apps need to handle passwords and other short but sensitive bits of data, such as keys and login tokens. The iOS keychain provides a secure way to store these items.

The keychain is implemented as a SQLite database stored on the file system. There is only one database; the *securityd* daemon determines which keychain items each process or app can access. Keychain access APIs result in calls to the daemon, which queries the app's "keychain-access-groups" and the "application-identifier" entitlement. Rather than limiting access to a single process, access groups allow keychain items to be shared between apps.

Keychain items can only be shared between apps from the same developer. This is managed by requiring third-party apps to use access groups with a prefix allocated to them through the iOS Developer Program. The prefix requirement is enforced through code signing and Provisioning Profiles.

Keychain data is protected using a class structure similar to the one used in file Data Protection. These classes have behaviors equivalent to file Data Protection classes, but use distinct keys and are part of APIs that are named differently.

Availability	File Data Protection	Keychain Data Protection
When unlocked	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
While locked	NSFileProtectionCompleteUnlessOpen	N/A
After first unlock	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Always	NSFileProtectionNone	kSecAttrAccessibleAlways

Apps that utilize background refresh services in iOS 7 are required to use `kSecAttrAccessibleAfterFirstUnlock` for keychain items that need to be accessed during background updates.

Each keychain class has a "This device only" counterpart, which is always protected with the UID when being copied from the device during a backup, rendering it useless if restored to a different device.

Apple has carefully balanced security and usability by choosing keychain classes that depend on the type of information being secured and when it's needed by the OS. For example, a VPN certificate must always be available so the device keeps a continuous connection, but it's classified as "non-migratory," so it can't be moved to another device.

For keychain items created by iOS, the following class protections are enforced:

Item	Accessible
Wi-Fi passwords	After first unlock
Mail accounts	After first unlock
Exchange accounts	After first unlock
VPN certificates	Always, non-migratory
VPN passwords	After first unlock
LDAP, CalDAV, CardDAV	After first unlock
Social network account tokens	After first unlock
Home sharing password	When unlocked
Find My iPhone token	Always
iTunes backup	When unlocked, non-migratory
Voicemail	Always
Safari passwords	When unlocked
Bluetooth keys	Always, non-migratory
Apple Push Notification Service Token	Always, non-migratory
iCloud certificates and private key	Always, non-migratory
iCloud token	After first unlock
iMessage keys	Always, non-migratory
Certificates and private keys installed by Configuration Profile	Always, non-migratory
SIM PIN	Always, non-migratory

Keybags

The keys for both file and keychain Data Protection classes are collected and managed in keybags. iOS uses the following four keybags: System, Backup, Escrow, and iCloud Backup.

System keybag is where the wrapped class keys used in normal operation of the device are stored. For example, when a passcode is entered, the `NSFileProtectionComplete` key is loaded from the system keychain and unwrapped. It is a binary plist stored in the No Protection class, but whose contents are encrypted with a key held in Effaceable Storage. In order to give forward security to keybags, this key is wiped and regenerated each time a user changes a passcode. The System keybag is the only keybag stored on the device. The `AppleKeyStore` kernel extension manages the System keybag, and can be queried regarding a device's lock state. It reports that the device is unlocked only if all the class keys in the System are accessible, having been unwrapped successfully.

Backup keybag is created when an encrypted backup is made by iTunes and stored on the computer to which the device is backed up. A new keybag is created with a new set of keys, and the backed-up data is re-encrypted to these new keys. As explained earlier, non-migratory keychain items remain wrapped with the UID-derived key, allowing them to be restored to the device they were originally backed up from, but rendering them inaccessible on a different device.

The keybag is protected with the password set in iTunes, run through 10,000 iterations of PBKDF2. Despite this large iteration count, there's no tie to a specific device, and therefore a brute-force attack parallelized across many computers can be attempted on the Backup keybag. This threat can be mitigated with a sufficiently strong password.

If a user chooses to not encrypt an iTunes backup, the backup files are not encrypted regardless of their Data Protection class, but the keychain remains protected with a UID-derived key. This is why keychain items migrate to a new device only if a backup password is set.

Escrow keybag is used for iTunes syncing and MDM. This keybag allows iTunes to back up and sync without requiring the user to enter a passcode, and it allows an MDM server to remotely clear a user's passcode. It is stored on the computer that's used to sync with iTunes, or on the MDM server that manages the device.

The Escrow keybag improves the user experience during device synchronization, which potentially requires access to all classes of data. When a passcode-locked device is first connected to iTunes, the user is prompted to enter a passcode. The device then creates an Escrow keybag and passes it to the host. The Escrow keybag contains exactly the same class keys used on the device, protected by a newly generated key. This key is needed to unlock the Escrow keybag, and is stored on the device in the Protected Until First User Authentication class. This is why the device passcode must be entered before backing up with iTunes for the first time after a reboot.

iCloud Backup keybag is similar to the Backup keybag. All the class keys in this keybag are asymmetric (using Curve25519, like the Protected Unless Open Data Protection class), so iCloud backups can be performed in the background. For all Data Protection classes except No Protection, the encrypted data is read from the device and sent to iCloud. The corresponding class keys are protected by iCloud keys. The keychain class keys are wrapped with a UID-derived key in the same way as an unencrypted iTunes backup.

FIPS 140-2

The cryptographic modules in iOS 7 have been validated to comply with U.S. Federal Information Processing Standard (FIPS) 140-2 Level 1. This validates the integrity of cryptographic operations in Apple apps and third-party apps that properly utilize iOS cryptographic services. Bluetooth services have not been validated. For more information, see http://support.apple.com/kb/HT5808.

App Security

Apps are among the most critical elements of a modern OS security architecture. While apps provide amazing productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly.

Because of this, iOS provides layers of protection to ensure that apps are signed and verified, cannot execute malicious code, and are sandboxed to protect user data at all times. These elements provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps on iOS without impacting system integrity. And users can access these apps on their iOS devices without undue fear of viruses, malware, or unauthorized attacks.

App Code Signing

Once the iOS kernel has started, it controls which user processes and apps can be run. To ensure that all apps come from a known and approved source and have not been tampered with, iOS requires that all executable code be signed using an Apple-issued certificate. Apps provided with the device, like Mail and Safari, are signed by Apple. Third-party apps must also be validated and signed using an Apple-issued certificate. Mandatory code signing extends the concept of chain of trust from the OS to apps, and prevents third-party apps from loading unsigned code resources or using self-modifying code.

In order to develop and install apps on iOS devices, developers must register with Apple and join the iOS Developer Program. The real-world identity of each developer, whether an individual or a business, is verified by Apple before their certificate is issued. This certificate enables developers to sign apps and submit them to the App Store for distribution. As a result, all apps in the App Store have been submitted by an identifiable person or organization, serving as a deterrent to the creation of malicious apps. They have also been reviewed by Apple to ensure they operate as described and don't contain obvious bugs or other problems. In addition to the technology already discussed, this curation process gives customers confidence in the quality of the apps they buy.

Businesses also have the ability to write in-house apps for use within their organization and distribute them to their employees. Businesses and organizations can apply to the iOS Developer Enterprise Program (iDEP) with a D-U-N-S number. Apple approves applicants after verifying their identity and eligibility. Once an organization becomes a member of iDEP, it can register to obtain a Provisioning Profile that permits in-house apps to run on devices it authorizes. Users must have the Provisioning Profile installed in order to run the in-house apps. This ensures that only the organization's intended users are able to load the apps onto their iOS devices. In-house apps also check to ensure the signature is valid at runtime. Apps with an expired or revoked certificate will not run.

Unlike other mobile platforms, iOS does not allow users to install potentially malicious unsigned apps from websites, or run untrusted code. At runtime, code signature checks of all executable memory pages are made as they are loaded to ensure that an app has not been modified since it was installed or last updated.

Runtime Process Security

Once an app is verified to be from an approved source, iOS enforces security measures designed to prevent it from compromising other apps or the rest of the system.

All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using application programming interfaces (APIs) and services provided by iOS.

System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted as read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.

Access by third-party apps to user information and features such as iCloud is controlled using declared entitlements. Entitlements are key/value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon.

In addition, apps can only perform background processing through system-provided APIs. This enables apps to continue to function without degrading performance or dramatically impacting battery life. Apps can't share data directly with each other; sharing can be implemented only by both the receiving and sending apps using custom URL schemes, or through shared keychain access groups.

Address space layout randomization (ASLR) protects against the exploitation of memory corruption bugs. Built-in apps use ASLR to ensure that all memory regions are randomized upon launch. Randomly arranging the memory addresses of executable code, system libraries, and related programming constructs reduces the likelihood of many sophisticated exploits. For example, a return-to-libc attack attempts to trick a device into executing malicious code by manipulating memory addresses of the stack and system libraries. Randomizing the placement of these makes the attack far more difficult to execute, especially across multiple devices. Xcode, the iOS development environment, automatically compiles third-party programs with ASLR support turned on.

Further protection is provided by iOS using ARM's Execute Never (XN) feature, which marks memory pages as non-executable. Memory pages marked as both writable and executable can be used only by apps under tightly controlled conditions: The kernel checks for the presence of the Apple-only dynamic code-signing entitlement. Even then, only a single mmap call can be made to request an executable and writable page, which is given a randomized address. Safari uses this functionality for its JavaScript JIT compiler.

Data Protection in Apps

The iOS Software Development Kit (SDK) offers a full suite of APIs that make it easy for third-party and in-house developers to adopt Data Protection and ensure the highest level of protection in their apps. Data Protection is available for file and database APIs, including NSFileManager, CoreData, NSData, and SQLite.

As of iOS 7, third-party apps that do not opt-in to a specific data protection class receive Protected Until First User Authentication by default. For devices that were upgraded from an earlier release to iOS 7, apps that were already installed at the time of the upgrade continue to use No Protection unless they specifically adopt a specific Data Protection class.

Accessories

The Made for iPhone, iPod touch, and iPad (MFi) licensing program provides vetted accessory manufacturers access to the iPod Accessories Protocol (IAP) and the necessary supporting hardware components.

When an accessory communicates with an iOS device using a Lightning connector cable, or via Wi-Fi or Bluetooth, the device asks the accessory to prove it has been authorized by Apple by responding with an Apple-provided certificate, which is verified by the device. The device then sends a challenge, which the accessory must answer with a signed response. This process is entirely handled by a custom integrated circuit that Apple provides to approved accessory manufacturers and is transparent to the accessory itself.

Accessories can request access to different transport methods and functionality; for example, access to digital audio streams over the Lightning cable, or Siri hands-free mode over Bluetooth. The IC ensures that only approved devices are granted full access to the device. If an accessory does not provide authentication, its access is limited to analog audio and a small subset of serial (UART) audio playback controls.

AirPlay also utilizes the authentication IC to verify that receivers have been approved by Apple. AirPlay audio and video streams utilize the MFi-SAP (Secure Association Protocol), which encrypts communication between the accessory and device using ECDH key exchange (Curve25519) with 2048-bit RSA keys and AES-128 in CTR mode.

Network Security

In addition to the built-in safeguards Apple uses to protect data stored on iOS devices, there are many network security measures that organizations can take to keep information secure as it travels to and from an iOS device.

Mobile users must be able to access corporate networks from anywhere in the world, so it's important to ensure that they are authorized and their data is protected during transmission. iOS uses—and provides developer access to—standard networking protocols for authenticated, authorized, and encrypted communications. To accomplish these security objectives, iOS integrates proven technologies and the latest standards for both Wi-Fi and cellular data network connections.

On other platforms, firewall software is needed to protect open communication ports against intrusion. Because iOS achieves a reduced attack surface by limiting listening ports and removing unnecessary network utilities such as telnet, shells, or a web server, no additional firewall software is needed on iOS devices.

SSL, TLS

iOS supports Secure Socket Layer (SSL v3) as well as Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) and DTLS. Safari, Calendar, Mail, and other Internet applications automatically use these mechanisms to enable an encrypted communication channel between the device and network services. High-level APIs (such as CFNetwork) make it easy for developers to adopt TLS in their apps, while low-level APIs (SecureTransport) provide fine-grained control.

VPN

Secure network services like virtual private networking typically require minimal setup and configuration to work with iOS devices. iOS devices work with VPN servers that support the following protocols and authentication methods:

- Juniper Networks, Cisco, Aruba Networks, SonicWALL, Check Point, Palo Alto Networks, Open SSL, and F5 Networks SSL-VPN using the appropriate client app from the App Store. These apps provide user authentication for the built-in iOS support.
- Cisco IPSec with user authentication by Password, RSA SecurID or CRYPTOCard, and machine authentication by shared secret and certificates. Cisco IPSec supports VPN On Demand for domains that are specified during device configuration.
- L2TP/IPSec with user authentication by MS-CHAPV2 Password, RSA SecurID or CRYPTOCard, and machine authentication by shared secret.
- PPTP with user authentication by MS-CHAPV2 Password and RSA SecurID or CRYPTOCard.

iOS supports VPN On Demand for networks that use certificated-based authentication. IT policies specify which domains require a VPN connection by using a configuration profile.

iOS 7 introduces per-app VPN support, facilitating VPN connections on a much more granular basis. Mobile device management (MDM) can specify a connection for each managed app and/or specific domains in Safari. This helps ensure that secure data always goes to and from the corporate network—and that a user's personal data does not.

Wi-Fi

iOS supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses 128-bit AES encryption, giving users the highest level of assurance that their data remains protected when sending and receiving communications over a Wi-Fi network connection. With support for 802.1X, iOS devices can be integrated into a broad range of RADIUS authentication environments. 802.1X wireless authentication methods supported on iPhone and iPad include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP.

Bluetooth

Bluetooth support in iOS has been designed to provide useful functionality without unnecessary increased access to private data. iOS devices support Encryption Mode 3, Security Mode 4, and Service Level 1 connections. iOS supports the following Bluetooth profiles:

- Hands-Free Profile (HFP 1.5)
- Phone Book Access Profile (PBAP)
- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Personal Area Network Profile (PAN)
- Human Interface Device Profile (HID)

Support for these profiles varies by device. For more information, see http://support.apple.com/kb/ht3647.

Single Sign-on

iOS supports authentication to enterprise networks through single sign-on (SSO). SSO works with Kerberos-based networks to authenticate users to services they are authorized to access. SSO can be used for a range of network activities from secure Safari session to third-party apps.

iOS SSO utilizes SPNEGO tokens and the HTTP Negotiate protocol to work with Kerberos-based authentication gateways and Windows Integrated Authentication systems that support Kerberos tickets. SSO support is based on the open source Heimdal project.

The following encryption types are supported:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari supports SSO, and third-party apps that use standard iOS networking APIs can be whitelisted to also use it. To configure SSO, iOS supports a configuration profile payload that allows MDM servers to push down the necessary settings. This includes setting the user principal name (that is, the Active Directory user account) and Kerberos realm settings, as well as configuring which apps and/or Safari web URLs should be allowed to use SSO.

AirDrop Security

iOS devices that support AirDrop use Bluetooth Low-Energy (BTLE) and Apple-created peer-to-peer Wi-Fi technology to send files and information to nearby devices.

When a user enables AirDrop, a 2048-bit RSA identity is stored on the device. Additionally, an AirDrop identity hash is created based on the email addresses and phone numbers associated with the user's Apple ID.

When a user chooses AirDrop as the method for sharing an item, the device emits an AirDrop signal over BTLE. Other devices that are awake, in close proximity, and have AirDrop turned on detect the signal and respond with a shortened version of their owner's identity hash.

AirDrop is set to share with Contacts Only by default. Users can also choose if they want to be able to use AirDrop to share with Everyone or turn off the feature entirely. In Contacts Only mode, the received identity hashes are compared with hashes of people in the initiator's Contacts. If a match is found, the sending device creates a peer-to-peer Wi-Fi network and advertises an AirDrop connection using Bonjour. Using this connection, the receiving devices send their full identity hashes to the initiator. If the full hash still matches Contacts, the recipient's first name and photo (if present in Contacts) are displayed in the AirDrop sharing sheet.

When using AirDrop, the sending user selects who they want to share with. The sending device initiates an encrypted (TLS) connection with the receiving device, which exchanges their iCloud identity certificates. The identity in the certificates is verified against each user's Contacts. Then the receiving user is asked to accept the incoming transfer from the identified person or device. If multiple recipients have been selected, this process is repeated for each destination.

In the Everyone mode, the same process is used but if a match in Contacts is not found, the receiving devices are shown in the AirDrop sending sheet with a silhouette and with the device's name, as defined in Settings > General > About > Name.

The Wi-Fi radio is used to communicate directly between devices without using any Internet connection or Wi-Fi Access Point.

Internet Services

Apple has built a robust set of services to help users get even more utility and productivity out of their devices, including iMessage, FaceTime, Siri, iCloud, iCloud Backup, and iCloud Keychain.

These Internet services have been built with the same security goals that iOS promotes throughout the platform. These goals include secure handling of data, whether at rest on the device or in transit over wireless networks; protection of users' personal information; and threat protection against malicious or unauthorized access to information and services. Each service uses its own powerful security architecture without compromising the overall ease of use of iOS.

iMessage

Apple iMessage is a messaging service for iOS devices and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification Service (APNs). Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data.

When a user turns on iMessage, the device generates two pairs of keys for use with the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key for signing. For each key pair, the private keys are saved in the device's keychain and the public keys are sent to Apple's directory service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

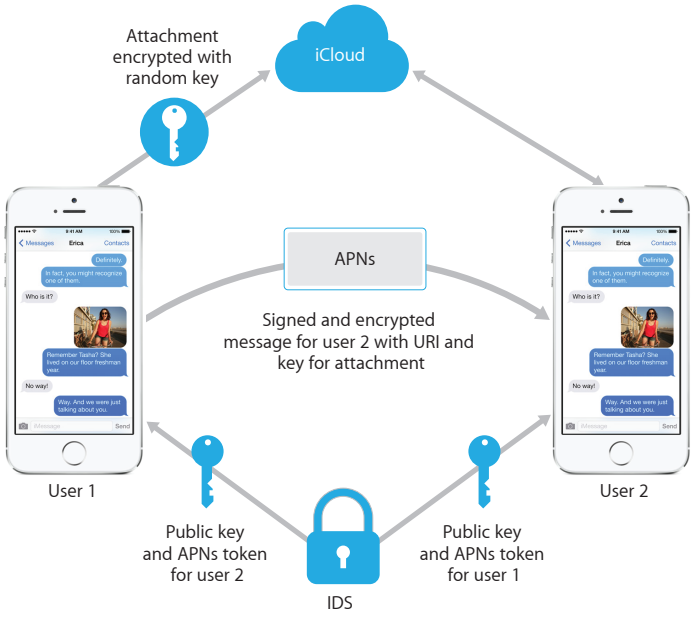
As users enable additional devices for use with iMessage, their public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which will be verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. Further, all of the user's registered devices display an alert message when a new device, phone number, or email address is added.

How iMessage sends and receives messages

Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the IDS to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. If the user enters a name, the device first utilizes the user's Contacts to gather the phone numbers and email addresses associated with that name, then gets the public keys and APNs addresses from the IDS.

The user's outgoing message is individually encrypted using AES-128 in CTR mode for each of the recipient's devices, signed using the sender's private key, and then dispatched to the APNs for delivery. Metadata, such as the timestamp and APNs routing information, is not encrypted. Communication with APNs is encrypted using TLS.

If the message text is too long, or if an attachment such as a photo is included, the attachment is encrypted using a random key and uploaded to iCloud. The key and URI (Uniform Resource Identifier) for the attachment are encrypted and signed, as shown below.



For group conversations, this process is repeated for each recipient and their devices.

On the receiving side, each device receives its copy of the message from APNs, and, if necessary, retrieves the attachment from iCloud. The incoming phone number or email address of the sender is matched to the receiver's Contacts so that a name can be displayed, if possible.

As with all push notifications, the message is deleted from APNs when it is delivered. Unlike other APNs notifications, however, iMessages are queued for delivery to offline devices. Messages are stored for up to seven days.

FaceTime

FaceTime is Apple's video and audio calling service. Similar to iMessage, FaceTime calls also use the Apple Push Notification Service to establish an initial connection to the user's registered devices. The audio/video contents of FaceTime calls are protected by end-to-end encryption, so no one but the sender and receiver can access them. Apple cannot decrypt the data.

FaceTime uses Internet Connectivity Establishment (ICE) to establish a peer-to-peer connection between devices. Using Session Initiation Protocol (SIP) messages, the devices verify their identity certificates and establish a shared secret for each session. The nonces supplied by each device are combined to salt keys for each of the media channels, which are streamed via Secure Real Time Protocol (SRTP) using AES-256 encryption.

Siri

By simply talking naturally, users can enlist Siri to send messages, schedule meetings, place phone calls, and more. Siri uses speech recognition, text-to-speech, and a client-server model to respond to a broad range of requests. The tasks that Siri supports have been designed to ensure that only the absolute minimal amount of personal information is utilized and that it is fully protected.

When Siri is turned on, the device creates random identifiers for use with the voice recognition and Siri servers. These identifiers are used only within Siri and are utilized to improve the service. If Siri is subsequently turned off, the device will generate a new random identifier to be used if Siri is turned back on.

In order to facilitate Siri's features, some of the user's information from the device is sent to the server. This includes information about the music library (song titles, artists, and playlists), the names of Reminders lists, and names and relationships that are defined in Contacts. All communication with the server is over HTTPS.

When a Siri session is initiated, the user's first and last name (from Contacts), along with a rough geographic location, is sent to the server. This is so Siri can respond with the name or answer questions that only need an approximate location, such as those about the weather. If a more precise location is necessary, perhaps to determine the location of nearby movie theaters for example, the server asks the device to provide a more exact location. This is an example of how, by default, information is sent to the server only when it's strictly necessary in order to process the user's request. In any event, session information is discarded after 10 minutes of inactivity.

The recording of the user's spoken words is sent to Apple's voice recognition server. If the task involves dictation only, the recognized text is sent back to the device. Otherwise, Siri analyzes the text and, if necessary, combines it with information from the profile associated with the device. For example, if the request is "send a message to my mom," the relationships and names that were uploaded from Contacts are utilized. The command for the identified action is then sent back to the device to be carried out.

Many Siri functions are accomplished by the device, under the direction of the server. For example, if the user asks Siri to read an incoming message, the server simply tells the device to speak the contents of its unread messages. The contents and sender of the message are not sent to the server.

User voice recordings are saved for a six-month period so that the recognition system can utilize them to better understand the user's voice. After six months, another copy is saved, without its identifier, for use by Apple in improving and developing Siri for up to two years. Additionally, some recordings that reference music, sports teams and players, and businesses or points of interest are similarly saved for purposes of improving Siri.

iCloud

iCloud stores music, photos, apps, calendars, documents, and more, and automatically pushes them to all of a user's devices. iCloud can also be used by third-party apps to store and sync documents as well as key values for app data as defined by the developer. An iCloud account is configured via the Settings app by the user. iCloud features, including Photo Stream, Documents & Data, and Backup, can be disabled by IT administrators via a configuration profile.

The service is agnostic about what is being stored and handles all files the same way. There are two components for each file. The first is the file's metadata, which consists of its name, extension, and filesystem permission settings. The second component is the file's contents, which are treated by iCloud simply as a collection of bytes.

Each file is broken into chunks and encrypted by iCloud using AES-128 and a key derived from each chunk's contents that utilizes SHA-256. The keys, and the file's metadata, are stored by Apple in the user's iCloud account. The encrypted chunks of the file are stored, without any user-identifying information, using third-party storage services, such as Amazon S3 and Windows Azure.

iCloud Backup

iCloud also backs up information—including device settings, app data, and text and MMS messages—daily over Wi-Fi. iCloud secures the content by encrypting it when sent over the Internet, storing it in an encrypted format, and using secure tokens for authentication. iCloud Backup occurs only when the device is locked, connected to a power source, and has Wi-Fi access to the Internet. Because of the encryption used in iOS, the system is designed to keep data secure while allowing incremental, unattended backup and restoration to occur.

Here's what iCloud backs up:

- Information about purchased music, movies, TV shows, apps, and books, but not the purchased content itself
- Photos and videos in Camera Roll
- Device settings
- App data
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Ringtones
- Visual Voicemail

When files are created in Data Protection classes that are not accessible when the device is locked, their per-file keys are encrypted using the class keys from the iCloud Backup keybag. Files are backed up to iCloud in their original, encrypted state. Files in Data Protection class No Protection are encrypted during transport as described in iCloud, above.

The iCloud Backup keybag contains asymmetric (Curve25519) keys for each Data Protection class, which are used to encrypt the per-file keys. For more information about the contents of the Backup keybag and the iCloud Backup keybag, see "Keychain Data Protection" in the Encryption and Data Protection section.

Safari integration with iCloud Keychain
Safari can automatically generate cryptographically strong random strings for website passwords, which are stored in Keychain and synced to your other devices. Keychain items are transferred from device to device, traveling through Apple servers, but are encrypted in such a way that Apple and other devices cannot read their contents.

The backup set is stored in the user's iCloud account and consists of a copy of the user's files, and the iCloud Backup keybag. The iCloud Backup keybag is protected by a random key, which is also stored with the backup set. (The user's iCloud password is not utilized for encryption so that changing the iCloud password won't invalidate existing backups.)

While the user's keychain database is backed up to iCloud, it remains protected by a UID-tangled key. This allows the keychain to be restored only to the same device from which it originated, and it means no one else, including Apple, can read the user's keychain items.

On restore, the backed-up files, iCloud Backup keybag, and the key for the keybag are retrieved from the user's iCloud account. The iCloud Backup keybag is decrypted using its key, then the per-file keys in the keybag are used to decrypt the files in the backup set, which are written as new files to the filesystem, thus re-encrypting them as per their Data Protection class.

iCloud Keychain

iCloud Keychain allows users to securely sync their passwords between iOS devices and Mac computers without exposing that information to Apple. In addition to strong privacy and security, other goals that heavily influenced the design and architecture of iCloud Keychain were ease of use and the ability to recover a keychain. iCloud Keychain consists of two services, keychain syncing and keychain recovery.

Apple designed iCloud Keychain and Keychain Recovery so that a user's passwords are still protected under the following conditions:

- A user's iCloud account is compromised.
- iCloud is compromised by an external attacker or employee.
- Third-party access to user accounts.

Keychain syncing

When a user enables iCloud Keychain for the first time, the device establishes a circle of trust and creates a syncing identity for itself. A syncing identity consists of a private key and a public key. The public key of the syncing identity is put in the circle, and the circle is signed twice: first by the private key of the syncing identity, then again with an asymmetric elliptical key (using P256) derived from the user's iCloud account password. Also stored with the circle are the parameters (random salt and iterations) used to create the key that is based on the user's iCloud password.

The signed syncing circle is placed in the user's iCloud key value storage area. It cannot be read without knowing the user's iCloud password, and cannot be modified without having the private key of the syncing identity of its member.

When the user turns on iCloud Keychain on another device, the new device notices in iCloud that the user has a previously established syncing circle that it is not a member of. The device creates its syncing identity key pair, then creates an application ticket to request membership in the circle. The ticket consists of the device's public key of its syncing identity, and the user is asked to authenticate with their iCloud password. The elliptical key generation parameters are retrieved from iCloud and generate a key that is used to sign the application ticket. Finally, the application ticket is placed in iCloud.

When the first device sees that an application ticket has arrived, it displays a notice for the user to acknowledge that a new device is asking to join the syncing circle. The user enters their iCloud password, and the application ticket is verified as signed by a matching private key. This establishes that the person who generated the request to join the circle entered the user's iCloud password at the time the request was made.

Upon the user's approval to add the new device to the circle, the first device adds the public key of the new member to the syncing circle, signs it again with both its syncing identity and the key derived from the user's iCloud password. The new syncing circle is placed in iCloud, where it is similarly signed by the new member of the circle.

How keychain syncing works

There are now two members of the signing circle, and each member has the public key of its peer. They now begin to exchange individual keychain items via iCloud key value storage. If both circle members have the same item, the one with the most recent modification date will be synced. Items are skipped if the other member has the item and the modification dates are identical. Each item that is synced is encrypted specifically for the device it is being sent to. It cannot be decrypted by other devices or Apple. Additionally, the encrypted item is ephemeral in iCloud; it's overwritten with each new item that's synced.

This process is repeated as new devices join the syncing circle. For example, when a third device joins, the confirmation appears on both of the other members. The user can approve the new member from either of those devices. As new peers are added, each peer syncs with the new one to ensure that all members have the same keychain items.

However, the entire keychain is not synced. Some items are device-specific, such as VPN identities, and shouldn't leave the device. Only items with the attribute `kSecAttrSynchronizable` are synced. Apple has set this attribute for Safari user data (including user names, passwords, and credit card numbers), as well as Wi-Fi passwords.

Additionally, by default, keychain items added by third-party apps do not sync. Developers must set the `kSecAttrSynchronizable` when adding items to the keychain.

Keychain recovery

Keychain recovery provides a way for users to optionally escrow their keychain with Apple, without allowing Apple to read the passwords and other data it contains. Even if the user has only a single device, keychain recovery provides a safety net against data loss. This is particularly important when Safari is used to generate random, strong passwords for web accounts, as the only record of those passwords is in the keychain.

A cornerstone of keychain recovery is secondary authentication and a secure escrow service, created by Apple specifically to support this feature. The user's keychain is encrypted using a strong passcode, and the escrow service will provide a copy of the keychain only if a strict set of conditions are met.

When iCloud Keychain is turned on, the user is asked to create an iCloud Security Code. This code is required to recover an escrowed keychain. By default, the user is asked to provide a simple four-digit value for the security code. However, users can also specify their own, longer code, or let their devices create a cryptographically random code that they can record and keep on their own.

Next, the iOS device exports a copy of the user's keychain, encrypts it with a random key, and places it in the user's iCloud key value storage area. The random key used to encrypt the keychain is wrapped with the user's iCloud Security Code and the public key of the HSM (hardware security module) cluster that will store the escrow record. This becomes the user's iCloud Escrow Record.

If the user decided to accept a cryptographically random security code, instead of specifying their own or using a four-digit value, no escrow record is necessary. Instead, the iCloud Security Code is used to wrap the random key directly.

In addition to establishing a security code, users must register a phone number. This is used to provide a secondary level of authentication during keychain recovery. The user will receive an SMS that must be replied to in order for the recovery to proceed.

Escrow security

iCloud provides a secure infrastructure for keychain escrow that ensures only authorized users and devices can perform a recovery. Topographically positioned behind iCloud are clusters of hardware security modules (HSM). These clusters guard the escrow records. Each has a key that is used to encrypt the escrow records under their watch, as described previously.

To recover a keychain, the user must authenticate with their iCloud account and password and respond to an SMS sent to their registered phone number. Once this is done, the user must enter their iCloud Security Code. The HSM cluster verifies that the user knows their iCloud Security Code using Secure Remote Password protocol (SRP); the

code itself is not sent to Apple. Each member of the cluster independently verifies that the user has not exceeded the maximum number of attempts that are allowed to retrieve their record, as discussed below. If a majority agree, the cluster unwraps the escrow record and sends it to the user's device.

Next, the device uses the iCloud Security Code to unwrap the random key used to encrypt the user's keychain. With that key, the keychain—retrieved from iCloud key value storage—is decrypted and restored onto the device. Only 10 attempts to authenticate and retrieve an escrow record are allowed. After several failed attempts, the record is locked and the user must call Apple Support to be granted more attempts. After the 10th failed attempt, the HSM cluster destroys the escrow record and the keychain is lost forever. This provides protection against a brute-force attempt to retrieve the record, at the expense of sacrificing the keychain data in response.

These policies are coded in the HSM firmware. The administrative access cards that permit the firmware to be changed have been destroyed. Any attempt to alter the firmware or access the private key will cause the HSM cluster to delete the private key. Should this occur, the owners of all keychains protected by the cluster will receive a message informing them that their escrow record has been lost. They can then choose to re-enroll.

Device Controls

iOS supports flexible security policies and configurations that are easy to enforce and manage. This enables organizations to protect corporate information and ensure that employees meet enterprise requirements, even if they are using devices they've provided themselves—for example, as part of a "bring your own device" (BYOD) program.

Organizations can use resources such as passcode protection, configuration profiles, remote wipe, and third-party MDM solutions to manage fleets of devices and help keep corporate data secure, even when employees access this data on their personal iOS devices.

Passcode Protection

In addition to providing the cryptographic protection discussed earlier, passcodes prevent unauthorized access to the device's UI. The iOS interface enforces escalating time delays after the entry of an invalid passcode, dramatically reducing the effectiveness of brute-force attacks via the Lock screen. Users can choose to have the device automatically wiped if the passcode is entered incorrectly after 10 consecutive attempts. This setting is available as an administrative policy and can also be set to a lower threshold through MDM and Exchange ActiveSync.

By default, the user's passcode can be defined as a four-digit PIN. Users can specify a longer, alphanumeric passcode by turning on Settings > General > Passcode > Complex Passcode. Longer and more complex passcodes are harder to guess or attack, and are recommended for enterprise use.

Administrators can enforce complex passcode requirements and other policies using MDM or Exchange ActiveSync, or by requiring users to manually install configuration profiles. The following passcode policies are available:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Auto-lock timeout
- Grace period for device lock
- Maximum number of failed attempts
- Allow Touch ID

For details about each policy, see the Configuration Profile Key Reference documentation at https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/.

Configuration Enforcement

A configuration profile is an XML file that allows an administrator to distribute configuration information to iOS devices. Settings that are defined by an installed configuration profile can't be changed by the user. If the user deletes a configuration profile, all the settings defined by the profile are also removed. In this manner, administrators can enforce settings by tying policies to access. For example, a configuration profile that provides an email configuration can also specify a device passcode policy. Users won't be able to access mail unless their passcodes meet the administrator's requirements.

An iOS configuration profile contains a number of settings that can be specified:

- Passcode policies
- Restrictions on device features (disabling the camera, for example)
- Wi-Fi settings
- VPN settings
- Email server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips
- Credentials and keys
- Advanced cellular network settings

Configuration profiles can be signed and encrypted to validate their origin, ensure their integrity, and protect their contents. Configuration profiles are encrypted using CMS (RFC 3852), supporting 3DES and AES-128.

Configuration profiles can also be locked to a device to completely prevent their removal, or to allow removal only with a passcode. Since many enterprise users own their iOS devices, configuration profiles that bind a device to an MDM server can be removed—but doing so will also remove all managed configuration information, data, and apps.

Users can install configuration profiles directly on their devices using Apple Configurator, or they can be downloaded via email or over the air using an MDM server.

Mobile Device Management (MDM)

iOS support for MDM allows businesses to securely configure and manage scaled iPhone and iPad deployments across their organizations. MDM capabilities are built on existing iOS technologies such as configuration profiles, over-the-air enrollment, and the Apple Push Notification Service. Using MDM, IT departments can enroll iOS devices in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed devices. For more information on mobile device management, visit www.apple.com/iphone/business/it/management.html.

Apple Configurator

In addition to MDM, Apple Configurator for OS X makes it easy for anyone to deploy iOS devices. Apple Configurator can be used to quickly configure large numbers of devices with the settings, apps, and data. Devices that are initially configured using Apple Configurator can be "supervised," enabling additional settings and restrictions to be installed. Once a device is supervised with Apple Configurator, all available settings and restrictions can be installed over the air via MDM as well. For more information on configuring and managing devices using both Apple Configurator and MDM, refer to *Deploying iPhone and iPad: Apple Configurator*.

Device Restrictions

Administrators can restrict device features by installing a configuration profile. The following restrictions are available:

- Allow app installs
- Allow use of camera
- Allow FaceTime
- Allow screen capture
- Allow voice dialing
- Allow automatic sync while roaming
- Allow in-app purchases
- Allow syncing of Mail recents
- Force user to enter store password for all purchases
- Allow multiplayer gaming
- Allow adding Game Center friends
- Allow Siri
- Allow Siri while device is locked
- Allow use of YouTube
- Allow Passbook notifications while device is locked
- Allow use of iTunes Store
- Allow use of Safari
- Enable Safari autofill
- Force Fraudulent Website Warning
- Enable JavaScript
- Block pop-ups
- Accept cookies
- Allow iCloud backup
- Allow iCloud document and key-value sync
- Allow Photo Streams
- Allow Shared Photo Streams
- Allow diagnostics to be sent to Apple
- Allow user to accept untrusted TLS certificates
- Force encrypted backups
- Restrict media by content rating
- Allow Touch ID
- Allow Control Center access from Lock screen
- Allow Today view from Lock screen

Supervised Only Restrictions

- Allow iMessage
- Allow Game Center
- Allow iBooks Store
- Allow erotica from iBooks Store
- Allow removal of apps
- Enable Siri Profanity Filter
- Allow manual install of configuration profiles
- Allow installation of configuration profiles
- Global network proxy for HTTP
- Allow pairing to computers for content sync
- Restrict AirPlay connections with whitelist and optional connection passcodes
- Allow AirDrop
- Allow account modification
- Allow Cellular Data modification
- Allow Find My Friends
- Allow Host Pairing (iTunes)
- Allow Activation Lock

Remote Wipe

iOS devices can be erased remotely by an administrator or user. Instant remote wiping is achieved by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable. Remote wiping can be initiated by MDM, Exchange, or iCloud.

When remote wiping is triggered by MDM or iCloud, the device sends an acknowledgment and performs the wipe. For remote wiping via Exchange, the device checks in with the Exchange Server before performing the wipe.

Users can also wipe devices in their possession using the Settings app. And as mentioned, devices can be set to automatically wipe after a series of failed passcode attempts.

Conclusion

A Commitment to Security

From hardware to encryption to device access, each component of the iOS security platform provides organizations with the resources they need to build enterprise-grade security solutions. Together, these components give iOS its industry-leading security features without making the device difficult to use.

Apple uses a consistent, integrated security infrastructure throughout iOS and the iOS apps ecosystem. Hardware-based storage encryption provides instant remote wipe capabilities when a device is lost, and enables users to completely remove all corporate and personal information when a device is sold or transferred to another owner. Diagnostic information is also collected anonymously.

iOS apps designed by Apple are built with enhanced security in mind. Safari offers safe browsing with support for Online Certificate Status Protocol (OCSP), EV certificates, and certificate verification warnings. Mail leverages certificates for authenticated and encrypted email by supporting S/MIME. iMessage and FaceTime also provide client-to-client encryption.

For third-party apps, the combination of required code signing, sandboxing, and entitlements gives users solid protection against viruses, malware, and other exploits that compromise the security of other platforms. The App Store submission process works to further shield users from these risks by reviewing every iOS app before it's made available for sale.

To make the most of the extensive security features built into iOS, businesses are encouraged to review their IT and security policies to ensure that they are taking full advantage of the layers of security technology offered by this platform.

Apple maintains a dedicated security team to support all Apple products. The team provides security auditing and testing for products under development, as well as for released products. The Apple team also provides security tools and training, and actively monitors for reports of new security issues and threats. Apple is a member of the Forum of Incident Response and Security Teams (FIRST). To learn more about reporting issues to Apple and subscribing to security notifications, go to apple.com/support/security.

Apple is committed to incorporating proven encryption methods and creating modern mobile-centric privacy and security technologies to ensure that iOS devices can be used with confidence in any personal or corporate environment.

Glossary

Address space layout randomization (ASLR)	A technique employed by iOS to make the successful exploitation of a software bug much more difficult. By ensuring memory addresses and offsets are unpredictable, exploit code can't hard code these values. In iOS 5 and later, the position of all system apps and libraries are randomized, along with all third-party apps compiled as position-independent executables.
Apple Push Notification Service (APNs)	A worldwide service provided by Apple that delivers push notifications to iOS devices.
Boot ROM	The very first code executed by a device's processor when it first boots. As an integral part of the processor, it can't be altered by either Apple or an attacker.
Data Protection	File and keychain protection mechanism for iOS. It can also refer to the APIs that apps use to protect files and keychain items.
Device Firmware Upgrade (DFU)	A mode in which a device's Boot ROM code waits to be recovered over USB. The screen is black when in DFU mode, but upon connecting to a computer running iTunes, the following prompt is presented: "iTunes has detected an iPad in recovery mode. You must restore this iPad before it can be used with iTunes."
ECID	A 64-bit identifier that's unique to the processor in each iOS device. Used as part of the personalization process, it's not considered a secret.
Effaceable Storage	A dedicated area of NAND storage, used to store cryptographic keys, that can be addressed directly and wiped securely. While it doesn't provide protection if an attacker has physical possession of a device, keys held in Effaceable Storage can be used as part of a key hierarchy to facilitate fast wipe and forward security.
File system key	The key that encrypts each file's metadata, including its class key. This is kept in Effaceable Storage to facilitate fast wipe, rather than confidentiality.
Group ID (GID)	Like the UID but common to every processor in a class.
Hardware security module (HSM)	A specialized tamper-resistant computer that safeguards and manages digital keys.
iBoot	Code that's loaded by LLB, and in turn loads XNU, as part of the secure boot chain.
Identity Service (IDS)	Apple's directory of iMessage public keys, APNs addresses, and phone numbers and email addresses that are used to look up the keys and device addresses.
Integrated circuit (IC)	Also known as a microchip.

Keybag	A data structure used to store a collection of class keys. Each type (System, Backup, Escrow, or iCloud Backup) has the same format: • A header containing: – Version (set to 3 in iOS 5) – Type (System, Backup, Escrow, or iCloud Backup) – Keybag UUID – An HMAC if the keybag is signed – The method used for wrapping the class keys: tangling with the UID or PBKDF2, along with the salt and iteration count • A list of class keys: – Key UUID – Class (which file or keychain Data Protection class this is) – Wrapping type (UID-derived key only; UID-derived key and passcode-derived key) – Wrapped class key – Public key for asymmetric classes
Keychain	The infrastructure and a set of APIs used by iOS and third-party apps to store and retrieve passwords, keys, and other sensitive credentials.
Key wrapping	Encrypting one key with another. iOS uses NIST AES key wrapping, as per RFC 3394.
Low-Level Bootloader (LLB)	Code that's invoked by the Boot ROM, and in turn loads iBoot, as part of the secure boot chain.
Per-file key	The AES 256-bit key used to encrypt a file on the file system. The per-file key is wrapped by a class key and is stored in the file's metadata.
Provisioning Profile	A plist signed by Apple that contains a set of entities and entitlements allowing apps to be installed and tested on an iOS device. A development Provisioning Profile lists the devices that a developer has chosen for ad hoc distribution, and a distribution Provisioning Profile contains the app ID of an enterprise-developed app.
Ridge flow angle mapping	A mathematical representation of the direction and width of the ridges extracted from a portion of a fingerprint.
System on a chip (SoC)	An integrated circuit (IC) that incorporates multiple components into a single chip. The Secure Enclave is an SoC within Apple's A7 central processor.
Tangling	The process by which a user's passcode is turned into a cryptographic key and strengthened with the device's UID. This ensures that a brute-force attack must be performed on a given device, and thus is rate limited and cannot be performed in parallel. The tangling algorithm is PBKDF2, which uses AES as the pseudorandom function (PRF) with a UID-derived key.
Uniform Resource Identifier (URI)	A string of characters that identifies a web-based resource.
Unique ID (UID)	A 256-bit AES key that's burned into each processor at manufacture. It cannot be read by firmware or software, and is used only by the processor's hardware AES engine. To obtain the actual key, an attacker would have to mount a highly sophisticated and expensive physical attack against the processor's silicon. The UID is not related to any other identifier on the device including, but not limited to, the UDID.
XNU	The kernel at the heart of the iOS and OS X operating systems. It's assumed to be trusted, and enforces security measures such as code signing, sandboxing, entitlement checking, and ASLR.

EXHIBIT G

iCloud: Erase your device

Languages English

If your iOS device or Mac is lost or stolen, you can erase it if you set up Find My iPhone on the device before it was lost. If you have Family Sharing set up, you can erase your family members' devices, too. For more information, see the Apple Support article Family Sharing.

Important: Before you erase your device, try to locate it or play a sound on it. After you erase it, you can't use Find My iPhone to do either. You may still be able to locate your Mac if it's near a previously used Wi-Fi network.

Erase your device or a family member's device

1. Go to Find My iPhone on iCloud.com.

   If you don't see Find My iPhone on iCloud.com, your account just has access to iCloud web-only features. To gain access to other iCloud features, set up iCloud on your iOS device or Mac.

2. Click All Devices, then select the device you want to erase.

3. In the device's Info window, click Erase [device].

4. To erase:

   - An iOS device: Enter your Apple ID password or your family member's Apple ID password. If the device you're erasing has iOS 7 or later, enter a phone number and message. The number and message are displayed on the screen after the device is erased.

   - A Mac: Enter your Apple ID password or your family member's Apple ID password. Enter a passcode to lock the Mac (you need to use the passcode to unlock it), then enter a message. The message is displayed on the screen after the Mac is erased.

After you set a device to erase

- If your device is online, the remote erase begins. A confirmation email is sent to your Apple ID email address.

- If your device is offline, the remote erase begins the next time it's online.

- If you erase then find your iOS device, you can restore the information on the device using iCloud Backup (if backup was turned on before you erased it) or iTunes. For more information, see iCloud storage and backup overview, or the "Safety, handling, and support" section of the iOS user guide for iPhone, iPad, or iPod touch. For a device that doesn't use the latest iOS version, get the user guide for iPhone, iPad, or iPod touch from the Apple Support manuals website.

- If you erase then find your Mac, you can restore the information on the Mac using a Time Machine backup, if you have one. For more information, see the Apple Support article Recover your entire system. If you set an EFI firmware password on your Mac before it was lost, then erase it and later find it, you may need to take your Mac to an authorized repair center to unlock it before you can use it again.

If you erase your iPhone 6 or iPhone 6 Plus and you have credit and debit cards in Wallet for Apple Pay, Find My iPhone attempts to remove your cards immediately, even if your iPhone is offline. For more information, see the Apple Support article Use Wallet on your iPhone or iPod touch.

Note: If you don't expect to find your iPhone or iPad (Wi-Fi + cellular models), contact your wireless service provider to suspend service so you aren't responsible for phone calls or other charges.

Last Modified: Feb 11, 2016

Helpful? Yes No

68% of people found this helpful.

Additional Product Support Information

iCloud

Support

EXHIBIT H

Use a passcode with your iPhone, iPad, or iPod touch

Learn how to set, use, and change a passcode on your iOS device.

Set a passcode on your iOS device to help protect your data. Each time you turn on or wake your device, you'll need to unlock it with your passcode. If your device supports Touch ID, you can use your fingerprint instead of a passcode.

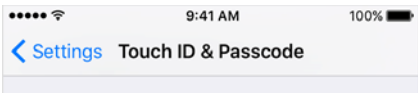
Here's when you'll enter your passcode:

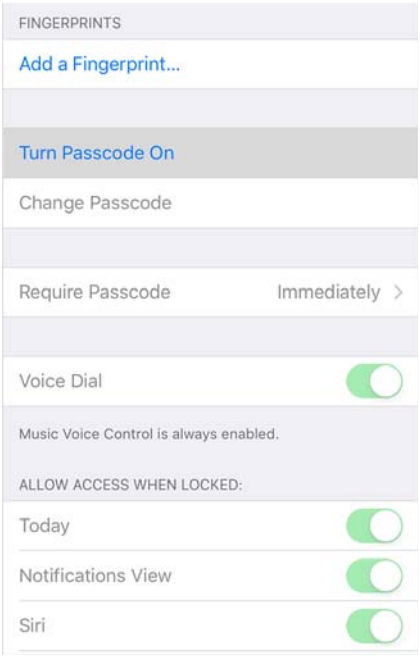
- Turn on or restart your device
- Slide to unlock your screen (you can change this)
- Update your software
- Erase your device

Set your passcode

1. Go to Settings > Touch ID & Passcode. On devices without Touch ID, go to Settings > Passcode:

2. Tap Turn Passcode On.

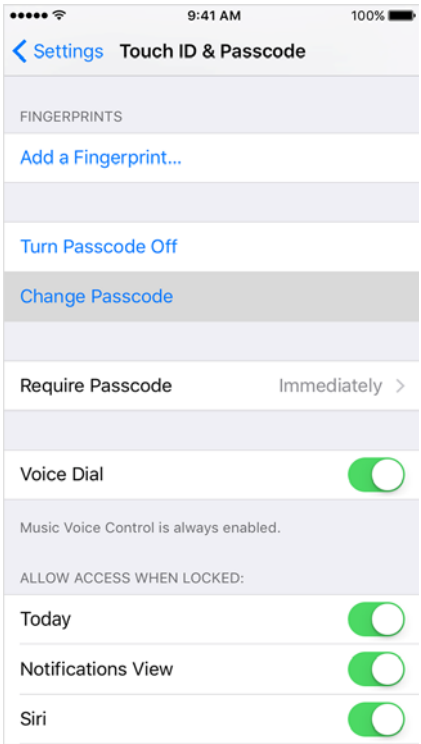




3. Enter a six-digit passcode. Or tap Passcode Options to switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code.
4. Enter your passcode again to confirm it and activate it.

Change your passcode or passcode settings

To change your passcode or passcode settings, go to Settings > Touch ID & Passcode. On devices without Touch ID, go to Settings > Passcode.



You'll find several settings and options:

- Turn Passcode Off.
- Change your passcode. Enter a new, six-digit passcode. Or tap Passcode Options to switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code.
- Require Passcode—Immediately: By default, as soon as you lock your screen, you'll need to enter your passcode to unlock it. If you don't want to need your passcode immediately, change this setting.
- Allow Access When Locked: Allow access to some features when your device is locked, including Notifications View, Siri, and Control Center.
- Erase Data: Choose whether to erase your device automatically after ten failed passcode attempts.

Can’t turn off your passcode or change passcode settings?

Passcode settings might be unavailable, gray, or dimmed. If you can't change these settings, it might be because you're using a configuration profile that requires a passcode. This is common with business or education devices. Contact your IT administrator for more information.

Forget your passcode?

If you or someone else enters the wrong passcode too many times, your device will disable itself temporarily. Get help if you forgot your passcode or your device is disabled.

Learn what to do if you forgot your Restrictions passcode.

Last Modified: Sep 16, 2015

Submit my question to the community

See all questions on this article See all questions I have asked

Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.
Get started