EMN:LHE/SK
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

No. 15-MC-1902 (JO)

– – – – – – – – – – – – – – – – – – – X

THE GOVERNMENT'S REPLY

ROBERT L. CAPERS
United States Attorney
Eastern District of New York

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

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

PRELIMINARY STATEMENT

A magistrate judge in the Eastern District of New York has issued a warrant to search an Apple iPhone 5s for evidence related to the possession and distribution of methamphetamine. The government has been unable to execute that warrant due to a passcode mechanism that prevents access to the phone's contents. The government conferred with Apple Inc. ("Apple"), and Apple confirmed, consistent with previous public statements, that it can bypass the lock screen for this device. Apple also provided the government with specific language to submit to the Court to obtain a lawful order for such a bypass.

On October 8, 2015, the government submitted an application to this Court, using Apple's requested language, for an Order under the All Writs Act, 28 U.S.C. § 1651, requiring Apple to assist in bypassing the lock screen of the phone. The application and proposed order (the "Application") are attached hereto as Exhibit A.[1]

On October 9, 2015, this Court entered a Memorandum and Opinion deferring the government's application and directing Apple to state whether bypassing the lock screen of the phone would be technically feasible and, if so, unduly burdensome to Apple (the "October 9 Order"). Apple submitted its response on October 19, 2015, confirming that it is technically feasible to bypass the lock screen of the phone, but claiming for the first time that assisting in the execution of the warrant could be unduly burdensome and could "tarnish the

[1] The application and proposed order have not been sealed and the government has not requested that they be filed under seal. Additionally, the underlying search warrant is publicly filed. See In re Cellular Telephone Devices Seized et al., No. 15-M-610 (E.D.N.Y. July 6, 2015).

Apple brand." Apple Br. at 4. The government now submits this brief in support of its Application and in reply to Apple's response.[2]

As set forth below, the government respectfully requests that this Court grant the government's Application and order Apple to assist with execution of the search warrant. The government seeks evidence relevant to a defendant's guilt in a federal criminal case and a magistrate judge has already determined that the government has a sufficient basis to search for such evidence on the defendant's phone. Absent Apple's assistance, the government cannot access that evidence without risking its destruction. But Apple can. Indeed, Apple has repeatedly assisted law enforcement officers in federal criminal cases by extracting data from passcode-locked iPhones pursuant to court orders. Apple has acknowledged that it has the technical capability to do so again in this case. It musters only two reasons not to compel its assistance now: it invokes the costs associated with devoting employee time to bypassing passcode-locked iPhones involved in criminal activity and potentially to testifying in federal court — costs that are minimal in comparison to the profits Apple has earned from marketing the same phones; and it invokes the prospect that offering assistance to the United States government in a federal criminal investigation, pursuant to an order from a United States federal court, would "tarnish the Apple brand." Apple's arguments are without basis as a matter of law.

[2] Apple has agreed to file a further reply in this matter on October 23rd. The United States is filing this reply at this time in order to help expedite this Court's resolution of this matter.

The government respectfully requests that this Court expedite its decision in this matter. The government seeks to obtain the evidence described in the underlying warrant in time to use it in a trial scheduled for November 16, 2015.[3]

[3] Either the United States or Apple may seek review of this Court's decision in the district court. In addition, should an order ultimately be issued to Apple directing its assistance in the matter, time will be required for Apple to perform a data extraction on the phone, for the government to search the data Apple is able to extract to locate evidence that falls within the scope of the warrant, including translating any evidence in a foreign language (as is expected in this case), and for the defense to review the evidence.

STATEMENT OF FACTS

The Apple iPhone 5s that is the subject of the government's application was seized pursuant to a search warrant from the residence of Jun Feng ("Feng"), a defendant in a criminal case. Feng has been indicted on three counts related to the possession and distribution of methamphetamine. See United States v. Jun Feng, No. 14-CR-387 (E.D.N.Y.). Trial is scheduled for November 16, 2015.

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 (the "Target Phone"). The next day, Drug Enforcement Administration ("DEA") agents inspected the Target Phone and determined that it was locked by a passcode. Later, the DEA agents consulted with personnel from the Federal Bureau of Investigation ("FBI"), and each agency agreed that neither could circumvent the passcode without risking data destruction.

Apple is the manufacturer of the iPhone Model 5s and the creator and licensor of the iOS operating system. The iOS operating system 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 the Target Phone — Apple has the technological capability to bypass the passcode feature and access the contents of the phone. 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, 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) (updated September 29, 2015), available at http://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf, attached hereto as Exhibit B. 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 applying for the order in this matter, the government consulted with Apple. 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. Apple's law enforcement liaison responded later that day and referred the government's inquiry to a colleague, an individual that Apple has specifically designated to handle routine law enforcement "data extraction" requests. Shortly thereafter, the referenced 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 the Target Phone was running an operating system that was "pre iOS 8," as the government had seized the Target Phone prior to the release of iOS 8. The government inquired, for a second time prior to seeking the proposed order, how long it would take for Apple to extract data from the phone. Later in the evening on October 7, 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, Apple provided the government with specific requests for the language it preferred in court orders and instructions for effectuating such an order. See Ex. B, § III(I).

The following day, on October 8, 2015, the government applied to this Court, serving as duty magistrate, for an order pursuant to the All Writs Act, directing Apple to extract the data from the passcode-locked Target Phone. With its application, the government submitted a proposed order that used the language that Apple requested in its Legal Process Guidelines.

After this Court issued the October 9 Order, the government served the Order upon Apple via email, sending it to Apple's central law enforcement email inbox as well as to the law enforcement liaison and data extraction specialist previously contacted. Later that

day, Apple's data extraction specialist responded and requested that the government provide a certain unique identifier associated with the Target Phone in order to validate which version of iOS software the Target Phone was running. On October 11, 2015, the government obtained the unique identifier Apple had requested from the investigative agent and provided it to Apple. Later that day, Apple informed the government that the Target Phone was indeed running an operating system that was pre iOS 8 — specifically, iOS 7. Apple then — again — provided the government with specific verbiage to be included in the proposed order submitted to the Court, which was the same verbiage contained in its previously-referenced Legal Process Guidelines. Apple still did not object to the government requesting such an order or indicate that complying with such an order would involve any burden.

Additional information from Apple revealed that the contents of the Target Phone were not backed up or otherwise copied onto Apple's iCloud cloud storage service and that the Target Phone had a remote wipe request pending. In other words, an individual had sent a command to the Target Phone directing the erasure of all of its contents. Therefore, if the Target Phone were connected to a network and powered on, the Target Phone would destroy the encryption keys necessary to decrypt the data on the phone, making it permanently inaccessible.

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, and the vast majority of these cases have been resolved

without any need for Apple to testify. In the course of handling these requests, Apple has, on multiple occasions, informed the government that it can extract data from a passcode-locked device and provided the government with the specific language it seeks in the form of a court order to do so. For example:

- 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 pled 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. Titus Lamar Bellot, No. 14-CR-48 (M.D. Fla. 2015).

- In one 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 pled guilty and was sentenced to twenty-three years' imprisonment. See United States v. Navarro, No. 13-CR-5525, ECF No. 52 (W.D. Wa. Dec. 16, 2013).

The government is not aware of any prior instance in which Apple objected to such an order.

ARGUMENT

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

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). In United States v. New York Telephone Co., 434 U.S. 159 (1977), the Supreme Court held that courts have authority under the All Writs Act to issue supplemental orders to third parties to facilitate the execution of search warrants. The Court held that "[t]he 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. In particular, the Court upheld an order directing a phone company to assist in executing a pen register search warrant issued under Rule 41. 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 iPhone search warrant.

Following New York Telephone Co., lower 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 1148, 1155 (3d Cir. 1979); In re Application, 616 F.2d 1122, 1129 (9th Cir. 1980).

- 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 In re Application of United States for an Order Directing X to Provide Access to Videotapes, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (hereinafter, "Access to Videotapes").
- Ordering a phone company to assist with consensual monitoring of a customer's calls. See In re Application, 2015 WL 5233551, at *4-5 (D.P.R. Aug. 27, 2015).

Significantly, in this exact context, another court held that the All Writs Act authorized the court to order the manufacturer to assist in extracting data from a cell phone through bypassing the passcode in order to execute a search warrant. See In re Order Requiring [XXX] to Assist in the Execution of a Search Warrant, 2014 WL 5510865, at *1-3 (S.D.N.Y. Oct. 31, 2014); see also United States v. Navarro, No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013). Moreover, the United States is not aware of any case since New York Telephone Co. in which the government obtained a Rule 41 search warrant but was unable to obtain an All Writs Act order to a company when necessary to facilitate the execution of the warrant.

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." Id. at 174. Second, it concluded that the order did not place an undue burden on the phone company. See id. at 175. Third, it determined that the assistance of the company was necessary to achieve the purpose of the warrant. See 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

First, Apple is not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." Apple designed, manufactured, and sold the Target Phone that is the subject of the search warrant. But that is only the beginning of Apple's relationship to the phone and to this matter. Apple wrote and owns the software that runs the phone, and this software is thwarting the execution of the warrant. 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." See "Notices from Apple," Apple iOS Software License Agreement ¶¶ B(1)-(2), attached hereto as Exhibit C. Apple also restricts users' rights to sell or lease 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." Ex. C, ¶ B(3). Apple cannot reap the legal benefits of licensing its software in this manner and then later disclaim

any ownership or obligation to assist law enforcement when that same software plays a critical role in thwarting execution of a search warrant.

Apple does not dispute that the iPhone's passcode mechanism is in part software-based; Apple notes that each device "includes both hardware and software security features." Apple Br. at 2. Apple's software impedes the execution of the search warrant in at least two ways. First, it includes the passcode feature that locks the Target Phone and prevents government access to stored information without further assistance from Apple. Second, Apple's software includes an "erase data" feature which, if enabled by the user, will render the data on the iPhone 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 Oct. 22, 2015), attached hereto as Exhibit D. This feature effectively prevents the government from attempting to execute the search warrant without Apple's assistance. In addition, through the iOS software, Apple provides other ongoing services to device owners, including one that may be used to thwart the execution of a search warrant: "erase your device" which allows a user to send a command remotely to erase data on an iPhone. See "iCloud: Erase your device," https://support.apple.com/kb/PH2701 (last visited Oct. 22, 2015), attached hereto as Exhibit E. As described above, in this case, someone sent an erase command to the Target Phone after the government seized the phone. Had the phone obtained a network connection while agents examined it, that erase command could have resulted in the data on the phone becoming permanently inaccessible. Given the role Apple's software plays in thwarting execution of the warrant, by preventing access and

permitting post-seizure deletion of data, Apple is not "so far removed from the underlying controversy that its assistance could not be permissibly compelled."

In its October 9 Order, this Court pointed out that unlike the company in New York Telephone Co., Apple is not "a highly regulated public utility with a duty to serve the public." But nothing in New York Telephone Co. suggests that this fact was essential to the Court's holding, and other courts have directed All Writs Act orders based on warrants to entities that are not public utilities. For example, neither the credit card company in Hall nor the landlord in Access to Videotapes were public utilities. See Hall, 583 F. Supp. at 722; Access to Videotapes, 2003 WL 22053105, at *3. Apple's close relationship to the iPhone and its software makes compulsion of Apple permissible, regardless of whether it is a public utility or whether it denies any duty to serve the public.

New York Telephone Co. emphasized that "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. By analogy, where Apple manufactured and sold a phone used in a criminal enterprise, where it owns and licensed the software used to further the criminal enterprise, where that very software now thwarts the execution of the search warrant, and where Apple provides ongoing services to phone owners, including the ability to wipe the phone remotely, compulsion of Apple is permissible under New York Telephone Co.

B. The order does not place an undue burden on Apple

Under New York Telephone Co., an All Writs Act order must not place an undue burden on Apple. See New York Telephone Co., 434 U.S. at 175. Here, Apple does not claim that assisting with the execution of the warrant would place on it an undue burden. It admits that it has previously bypassed passcode-locked devices in response to court orders, and it admits that doing so here "would not likely place a substantial financial or resource burden on Apple." Apple Br. at 3 & n.3. The Supreme Court in New York Telephone held that the All Writs Act order was not burdensome because it required minimal effort by the company and provided for reimbursement for the company's efforts. See id. Under this standard, Apple's admissions demonstrate that its assistance will not subject it to an undue burden.

Apple asserts that its burden "increases as the number of government requests increases," Apple Br. at 3, but it makes no attempt to quantify this burden or demonstrate that such orders have in fact cumulatively burdened it significantly. To the contrary, Apple demonstrates why any cumulative burden is minimal and likely to decrease with regard to the type of relief requested here: by its own measure, Apple retains the ability to bypass the passcode on only the 10% of its mobile devices that are "pre-iOS 8," and that number will continue to shrink as new devices are upgraded and replaced. See Apple Br. at 2. Nevertheless, the reasoning of New York Telephone Co. suggests that courts should not consider cumulative burden in assessing the burden from complying with a specific All Writs Act order: rather than consider the cumulative burden on phone companies of compliance with multiple pen register orders, the Supreme Court found that the district court's order was

not "in any way burdensome." New York Telephone Co., 434 U.S. at 175. In addition, any such burden on Apple is appropriately addressed by compensating Apple for its efforts in extracting data from the phone.

Similarly, Apple notes that it could potentially incur costs if its employees are later required to testify in court, but it again makes no attempt to quantify such costs or demonstrate an undue burden. Apple does not indicate how often it has been required to testify after extracting data from passcode-locked phones. The vast majority of cases in which Apple has assisted law enforcement by extracting data from passcode-locked iPhones have been resolved without any need for Apple to testify. This is because most criminal cases are resolved — by plea agreement or otherwise — prior to trial and, even in the event of a trial, the parties in a criminal case often reach stipulations obviating the need for such testimony. In any event, the reasoning of New York Telephone Co. suggests that fulfilling a duty to provide testimony does not create an undue burden on a provider, as the Court did not consider testimony when weighing the burden on the provider. Moreover, other companies and individuals — whether or not their involvement in a criminal case derives from a commercial connection to the evidence — bear the burden of providing court testimony on a regular basis; there is no reason to believe that this duty will unduly burden a corporation as large and wealthy as Apple, which according to its own public statements earns over $100 million in profits every day.[4] See Blair v. United States, 250 U.S. 273, 281 (1919) ("it is

[4] See "Apple Reports Record Third Quarter Results: iPhone, Apple Watch, Mac & App Store Drive Revenue Growth of 33%," https://www.apple.com/pr/library/2015/07/21Apple-Reports-Record-Third-Quarter-Results.html.

clearly recognized that the giving of testimony and the attendance upon court or grand jury in order to testify are public duties which every person within the jurisdiction of the government is bound to perform upon being properly summoned").

Finally, Apple points to its role in protecting customers' data "against any form of improper access," and it speculates that requiring its assistance "absent clear legal authority to do so[] could threaten the trust between Apple and its customers and substantially tarnish the Apple brand." Apple Br. at 4. These concerns do not establish an undue burden — or any legally cognizable burden at all — on Apple. In this case, the government seeks to search the Target Phone pursuant to a validly issued search warrant, and an All Writs Act order under New York Telephone Co. provides clear legal authority for requiring Apple's assistance. Therefore, this matter involves no "form of improper access" whatsoever. The requested access is legal and proper and, significantly, Apple does not claim an interest in preventing legal and proper access to data.

Apple's stated reputational concerns are particularly ill-founded in this case because Apple has previously publicly stated that it will extract data from phones running iOS versions before 8.0 when the government obtains a warrant. See Ex. B, § III(I). As the government's discussions with Apple before and after the issuance of the October 9 Order demonstrate, Apple has previously treated data extraction from passcode-locked phones pursuant to warrants as a routine duty when so required by a court. Apple cannot claim it faces an undue burden from complying with a court order requiring it to perform actions that it previously announced that it would perform.

Nor can Apple credibly claim to its potential customer base that it is not associated with the United States such that providing assistance in a federal criminal case, pursuant to a federal court order, would "tarnish" its brand. Apple is an American company, incorporated in California, and derives significant legal, infrastructural, and political benefits from that status. Apple owns thousands of patents registered in the United States, and thus relies on the American legal system to protect its valuable intellectual property. Apple makes frequent recourse to the American courts — including the United States federal courts, which issued the instant search warrant — to vindicate its property rights. It also frequently and voluntarily associates itself with American law enforcement, including federal law enforcement, when it believes that it has been a victim of a crime.

More generally, the burden associated with compliance with legal process is measured based on the direct costs of compliance, not on other more general considerations about reputations or the ramifications of compliance. For example, an All Writs Act order may be used to require the production of a handwriting exemplar, see United States v. Li, 55 F.3d 325, 329 (7th Cir. 1995), even though the subject may face criminal sanctions as a result of his compliance. Similarly, a gang member may face substantial reputational or economic consequences among his peers if he complies with a lawful order to testify against a fellow gang member, but such "harms" would not make an order to testify unduly burdensome. Apple's much more speculative concerns regarding possible reputational consequences from compliance with a court order in this matter merit no weight. In addition, complying with a court order based on a warrant serves the ends of justice and protects public safety. This Court should not entertain an argument that fulfilling basic civic responsibilities of any

American citizen or company — complying with a court order and testifying at trial — would "tarnish" that person's or company's reputation.

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) (emphasis added). In New York Telephone Co., the Court held that the 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. Here, 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 execute the warrant.

As an initial matter, Apple has confirmed its ability to bypass the passcode and extract data from the Target Phone in this case. Thus, it is clear that an All Writs Act Order will facilitate execution of the warrant.

The government could attempt to guess the Target Phone's passcode, but this technique is inadequate for two reasons. The phone may be configured to destroy data after ten unsuccessful attempts to guess the passcode. Even if it is not so configured, the government may be unable to guess a strong passcode in a reasonable amount of time.

This Court's October 9 order suggests that the government might attempt to compel Feng to unlock the Target Phone, see Order at 7, but that approach is also unworkable. Through counsel, Feng asserts that he has forgotten the passcode, which, if true, renders him unable to offer assistance.

Even if Feng knew the passcode, attempting to compel him to unlock the Target Phone would not provide an adequate alternative to an order directed to Apple. Compelled decryption raises significant Fifth Amendment issues and creates risk that the fruits of the compelled decryption could be suppressed. See, e.g., In re Grand Jury Subp. Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012) (holding that the Fifth Amendment protects a defendant's refusal to decrypt electronic storage media). The government should not be required to pursue a path for obtaining evidence that might lead to suppression. For example, in In re United States, 10 F.3d 931, 933 (2d Cir. 1993), the Second Circuit granted the government's writ of mandamus and directed a district court not to delegate review of Title III applications to a magistrate judge, as an appeal after the magistrate judge had reviewed the applications could have led to suppression. The court explained that the government "has a strong interest in ensuring the admissibility of evidence it gathers." Id. Thus, 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.

II. Congress has not limited this Court's authority to issue an All Writs Act order to Apple

A. No statute addresses data extraction from a passcode-locked cell phone

The Supreme Court also has made clear that "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute," such that courts may not rely on the All Writs Act "[w]here a statute specifically addresses the particular

issue at hand." Pennsylvania Bureau of Correction v. United States Marshals Serv., 474 U.S. 34, 43 (1985). In this case, no statute addresses the procedures for requiring Apple to extract data from a passcode-locked iPhone, so Pennsylvania Bureau of Correction provides no basis for denying the government's application for an All Writs Act order in this case.

This Court's October 9 Order references the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1002, but CALEA does not "specifically address" — or even vaguely address — the duty of Apple to assist in extracting data from a passcode-locked cell phone. CALEA requires telecommunications carriers to retain the capability to comply with court orders for real-time interceptions and call-identifying information (data "in motion").[5] Id. By contrast, this case involves evidence already stored on a cell phone (data "at rest"). Here, Apple is not acting as a telecommunications carrier, it already has the capability to implement the court order, and the court order concerns access to stored data rather than real-time interceptions and call-identifying information. Put simply, CALEA is entirely inapplicable to the present dispute. Moreover, even if it were applicable, CALEA addresses a provider's capability to produce information when it receives a court order, not the government's authority to obtain information pursuant to a court order in the first place. Thus, CALEA concerns a separate subject entirely and does not

[5] For example, for the contents of communications, CALEA requires telecommunications carriers to be able "to intercept" wire and electronic communications carried by the carrier. 47 U.S.C. § 1002(a)(1). CALEA incorporates the definition of "intercept" from the Wiretap Act, see 47 U.S.C. § 1001(1) & 18 U.S.C. § 2510(4), and that definition "encompasses only acquisitions contemporaneous with transmission." United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003).

limit this Court's authority under the All Writs Act to require Apple to assist the government in executing a search warrant.[6]

New York Telephone Co. further illustrates that it is appropriate for a court to rely on the All Writs Act unless a statute specifically addresses the particular issue at hand. When the Court decided New York Telephone Co. in 1977, Congress had enacted Title III for intercepting the contents of communications, but it had not yet enacted the closely-related pen register statute for acquiring 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. Under this reasoning, CALEA is no barrier to the issuance of an All Writs Act order requiring Apple to assist in decrypting an iPhone.

B. Congressional inaction does not deprive courts of their authority under the All Writs Act

Current Congressional attention to encryption-related issues does not deprive this Court of its authority to issue an assistance order to Apple. Under Pennsylvania Bureau

---

[6] Furthermore, nothing in CALEA prevents a court from ordering a telecommunications carrier to decrypt communications that it is capable of decrypting. See 47 U.S.C. § 1002(b)(3). When Congress enacted CALEA, it understood that existing provider-assistance provisions required a provider to decrypt communications when it was able to do so. Both the House and Senate reports for CALEA stated that "telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it." H.R. Rep. No. 103-827(I), at 24 (1994); S. Rep. No. 103-402, at 24 (1994) (emphasis added).

of Correction, courts may not rely on the All Writs Act where "a statute specifically addresses" an issue, not where Congress has declined to legislate. Court authority to issue All Writs Act orders in support of warrants has been clearly established since the Supreme Court decided New York Telephone Co. in 1977. Congress may choose to expand or limit this authority, but it must do so through enactment of legislation.

The Supreme Court and the Second Circuit have repeatedly cautioned that "Congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction." Zino Davidoff v. CVS, 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). Here, there are many possible explanations for congressional inaction on encryption, 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. These possibilities provide no basis for restricting legal authorities that existed before the beginning of the debate.[7] Because courts do not lose an authority to issue orders under the All Writs Act merely because Congress does not subsequently enact legislation endorsing or expanding that authority, this Court retains authority to issue an All Writs Act order consistent with New York Telephone Co.

[7] Granting legal force to statements or proposals by individual members of Congress during the course of Congressional debate risks absurd results. Congress routinely debates and fails to act on important issues, but the mere debate does not restrict existing legal authority. Under the Constitution, Congress speaks with legal force only when it speaks as one body, through bicameralism and presentment — i.e. when it passes a law.

In any event, the recent public and Congressional debate over encryption has not focused on the type of smartphone encryption at issue in this case, where the provider has publically acknowledged that it can bypass the encryption. Rather, it has focused on more recent software, such as Apple's iOS 8.0, which providers claim they cannot bypass. For example, the October 9 Order cites a July 6, 2015 article by FBI Director James Comey stating his concern that "in the not too distant future, . . . our conversations and our 'papers and effects' will be locked in such a way that permits access only by participants to a conversation or the owner of the device holding the data." See "Encryption, Public Safety, and 'Going Dark,'" LawFare, https://www.lawfareblog.com/encryption-public-safety-and-going-dark (July 6, 2015).

However, the order in this case would not require Apple to make any changes to its software or hardware, and it would not require Apple to introduce any new ability to access data on its phones. It would simply require Apple to use its existing capability to bypass the passcode on a passcode-locked iOS 7 phone, consistent with its previously stated public policy, and as it has routinely done so many times before. Moreover, it is hardly surprising that there has been little debate over whether the All Writs Act is available to order Apple to bypass a passcode-locked phone that it is capable of bypassing. That authority follows directly from New York Telephone Co., and every other federal court to consider this issue has directed Apple's assistance. See e.g., In re Order Requiring [XXX] to Assist in the Execution of a Search Warrant, 2014 WL 5510865, at *1-3 (S.D.N.Y. Oct. 31, 2014); Orders requiring Apple to assist law enforcement agents in the search of an Apple

iPhone 5 in advance of trial, United States v. Navarro, No. 13-CR-5525, ECF Nos. 39, 52 (W.D. Wa. Dec. 16, 2013).

The government has obtained a lawful search warrant for evidence of crime, but unless this Court issues the requested order, that warrant will be meaningless, and legitimate interests in public safety and the rule of law will be thwarted.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court issue the proposed order.

Dated: Brooklyn, New York
October 22, 2015

Respectfully submitted,

ROBERT L. CAPERS
United States Attorney

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

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

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