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)