UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Docket Nos. 14 Cr. 387 (MKB) 15 Misc. 1902 (JO)

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

Marc J. Zwillinger*
marc@zwillgen.com
Jeffrey G. Landis*
jeff@zwillgen.com
ZWILLGEN PLLC
1900 M Street N.W., Suite 250
Washington, D.C. 20036
Telephone: 202.706.5202
Facsimile: 202.706.5298

*Admitted *Pro Hac Vice*

Theodore J. Boutrous Jr.*
tboutrous@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

Alexander H. Southwell
asouthwell@gibsondunn.com
Mylan L. Denerstein
mdenerstein@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Attorneys for Apple Inc.

TABLE OF CONTENTS

TABLE OF CONTENTS
(*continued*)

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(*continued*)

Page(s)

TABLE OF AUTHORITIES
(*continued*)

Page(s)

TABLE OF AUTHORITIES
(*continued*)

Page(s)

TABLE OF AUTHORITIES
(*continued*)

Page(s)

Statutes

Other Authorities

TABLE OF AUTHORITIES
(*continued*)

Rules

I. PRELIMINARY STATEMENT

The government seeks to compel Apple to take possession of an iPhone and breach its security features absent any showing of the need for Apple's assistance, and under a sweeping interpretation of the All Writs Act that has been soundly rejected by Magistrate Judge Orenstein—an inconvenient fact the government attempts to obscure by styling its present application as a renewed application subject to *de novo* review. The government requests this extraordinary relief notwithstanding: the likely minimal evidentiary value of any data on the phone (given that all defendants have pled guilty and the phone was seized and last used nearly two years ago); that Congress has never authorized the power to compel private parties that the government seeks here; and that the record is devoid of evidence that Apple's assistance is necessary—and remains so even after a similar claim of necessity was proven untrue in a recent proceeding in California. Indeed, in its original application to Judge Orenstein, the government acknowledged that it sought Apple's help to spare *the government* from having to expend "significant resources." DE 1 at 2-3.[1] Moreover, the government has lodged this application even as members of Congress are debating the legality of these kinds of requests, and after FBI Director James Comey expressly observed that litigation is ill-suited for resolution of complex policy debates such as this. *See* Ex. A[2] [James Comey, *The Expectations of Privacy: Balancing Liberty, Security, and Public Safety*, Kenyon College (Apr. 6, 2016) (observing that "litigation is a terrible place to have any kind of discussion about a complicated policy issue, especially one that touches on our values, on the things we care about most, on technology, on tradeoffs and

[1] Unless otherwise noted, all references to docket entries ("DE") are to the docket in Case No. 15-mc-1902.

[2] All referenced exhibits are attached to the Declaration of Alexander H. Southwell, dated April 15, 2016, and filed concurrently herewith.

balance")]. For all of these reasons, Judge Orenstein's opinion should be affirmed, and the government's application should be denied.

As a preliminary matter, the government has utterly failed to satisfy its burden to demonstrate that Apple's assistance in this case is necessary—a prerequisite to compelling third party assistance under the All Writs Act. *See United States v. N.Y. Tel. Co.* ("*New York Telephone*"), 434 U.S. 159, 175 (1977). The government has made no showing that it has exhausted alternative means for extracting data from the iPhone at issue here, either by making a serious attempt to obtain the passcode from the individual defendant who set it in the first place—nor to obtain passcode hints or other helpful information from the defendant—or by consulting other government agencies and third parties known to the government. Indeed, the government has gone so far as to claim that it has no obligation to do so, *see* DE 21 at 8, notwithstanding media reports that suggest that companies already offer commercial solutions capable of accessing data from phones running iOS 7, which is nearly three years old. *See* Ex. B [Kim Zetter, *How the Feds Could Get into iPhones Without Apple's Help*, Wired (Mar. 2, 2016) (discussing technology that might be used to break into phones running iOS 7)]. Further undermining the government's argument that Apple's assistance is necessary in these proceedings is the fact that only two and a half weeks ago, in a case in which the government first insisted that it needed Apple to write new software to enable the government to bypass security features on an iPhone running iOS 9, the government ultimately abandoned its request after claiming that a third party could bypass those features *without Apple's assistance*. *See* Ex. C [*In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate #5KGD203* ("*In the Matter of the Search of an Apple iPhone*" or the "San Bernardino Matter"), No. 16-cm-10, DE 209 (C.D. Cal. Mar. 28,

2016)]. In response to those developments, the government filed a perfunctory letter in this case stating only that it would not modify its application. DE 39. The letter does not state that the government attempted the method that worked on the iPhone running iOS 9, consulted the third party that assisted with that phone, or consulted other third parties before baldly asserting that Apple's assistance remains necessary in these proceedings. *See id.* The government's failure to substantiate the need for Apple's assistance, alone, provides more than sufficient grounds to deny the government's application.

Apart from this fundamental deficiency, the government's request is predicated on a distortion of the All Writs Act. The government would have this Court believe that the All Writs Act, first enacted in 1789, is a boundless grant of authority that permits courts to enter any order the government seeks—including orders conscripting private third parties into providing whatever assistance law enforcement deems appropriate—as long as Congress has not expressly prohibited its issuance. DE 30 at 18. But that characterization of the All Writs Act turns our system of limited government on its head. It simply is not the case that federal courts can issue any order the executive branch dreams up unless and until Congress expressly prohibits it. That construction of the All Writs Act has it exactly backwards. If the government's view is correct, Congress would never need to pass permissive legislation in the law enforcement context because everything would be on the table until explicitly prohibited. That may be what the government prefers, but it is not the legal system in which it operates.

Moreover, the government's request contravenes congressional intent. Neither the Communications Assistance for Law Enforcement Act ("CALEA") nor the comprehensive legislative scheme of which it is a part authorizes the order the government seeks here; to the contrary, they collectively confirm that Congress never intended that such authority be available.

While Apple strongly supports, and will continue to support, the efforts of law enforcement in pursuing criminals, the government's sweeping interpretation of the All Writs Act is plainly incorrect and provides no limit to the orders the government could obtain in the future. And that is precisely what the government seeks here: to obtain an order that it can use as precedent to lodge future, more onerous requests for Apple's assistance, *see* DE 29 at 41 (noting that the government "clearly intends to continue seeking assistance that is similarly burdensome – if not more so – for the foreseeable future"); *see also* Ex. D [Spencer Ackerman & Sam Thielman, *FBI Director Admits Apple Encryption Case Could Set Legal Precedent*, Guardian (Feb. 25, 2016)], notwithstanding that the scope of the government's authority to compel third party assistance and the legality of these requests is currently the subject of ongoing political and public debate.[3] This Court should reject the government's overreaching and unsupported interpretation of the All Writs Act, and deny the government's application.

II. FACTUAL BACKGROUND

A. Apple's Device Security And Prior Extraction Orders.

Apple consistently strives to increase the security of its devices to protect the safety and privacy of its customers against threats known and unknown. Apple implemented strong

[3] *See, e.g.*, Ex. E [Hearing on Encryption Security and Privacy Before the H. Judiciary Comm. (Mar. 1, 2016) ("*Encryption Hr'g*")]; Ex. F [Hearing on World Wide Threats Before the H. Select Intelligence Comm. (Feb. 25, 2016)]. In addition, members of Congress have lodged several legislative proposals, some of which would require companies to assist the government, while others would prohibit compulsory assistance. *See* Ex. G [Sean Sposito & Carolyn Lochhead, *As Apple, FBI Spar, Feinstein Pushes Bill to Require Decryption*, SF Gate (Apr. 8, 2016) (describing draft legislation by Senators Dianne Feinstein and Richard Burr that would compel technology companies to assist government agencies in gaining access to encrypted technology)]; *see also* Secure Data Act of 2015, S.135, 114th Cong. (2015) (proposal to prohibit federal agencies from requiring hardware or software manufacturers to design or alter security functions in their products to allow surveillance, and exempting products used pursuant to CALEA); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015) (same); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015) (same, amending the Foreign Intelligence Surveillance Act of 1978).

encryption as far back as iOS 3, which was released in 2009, and with each update, has added new security features to better protect users' information from hackers and cyber criminals. In iOS 7, which is the operating system on the iPhone 5s at issue here, Apple, among other things, added Touch ID, introduced FaceTime audio encryption, and upgraded its "Find My iPhone" program to allow users to track, lock, and remotely wipe their lost or stolen phone. *See* Ex. H [Apple Inc., *iOS Security: iOS 9.0 or later* (Sept. 2015)]; *see also* Ex. I [Max Eddy, *iOS 7 Makes the iPhone More Secure than Ever*, PCMag.com (Sept. 13, 2013)]. Beginning with iOS 8, Apple introduced a feature that prevents anyone without the passcode from accessing the device's encrypted data, including Apple. *See generally* Ex. H [Apple Inc., *iOS Security: iOS 9.0 or later* (Sept. 2015)].

Apple does have the technical ability to extract unencrypted user data from a locked device running iOS 7 or earlier. *See* DE 11 at 3. Whether the extraction can be performed depends on the device, and whether it is in good working order. *Id.* As a general matter, certain user-generated active files on an iOS device that are contained in Apple's native apps can be extracted. *Id.* Apple cannot, however, extract email, calendar entries, or any other third-party app data. *Id.* Apple has in the past extracted unencrypted data from locked devices running iOS 7 or earlier and provided such data to the government in response to court orders. DE 16 at 3. In those cases, however, the government had obtained the order in *ex parte* proceedings in which Apple did not participate. *Id.*

B. The Drug Trafficking Case Against Jun Feng.

On June 6, 2014, in conjunction with an ongoing drug-trafficking investigation, the government obtained a warrant to search the residence of Jun Feng ("Feng"). *See United States v. The Premises Known and Described as 41-21 149th Street, 1st Floor, Queens, NY*, No. 14-MJ-530 (MDG), DE 2. During that search, the government seized an iPhone 5s running iOS 7

("Feng's iPhone"), the then-current operating system for iPhones. Law enforcement arrested Feng on June 11, 2014, and a grand jury indicted him on July 9, 2014, for conspiracy to traffic in methamphetamine. *See United States v. Yang*, No. 14-CR-387 (MKB), DE 25 (minute entry); DE 47 (indictment).

Not until more than a year after seizing Feng's iPhone did the government seek to search it. A search warrant application was granted on July 6, 2015. *See United States v. Cellular Tel. Devices Seized on or About June 11, 2014 from Premises Located at 41-21 149th Street, First Floor, in Queens, NY*, 15-MJ-610 (VVP), DE 1 (application for warrant). The government claims that the U.S. Drug Enforcement Agency ("DEA") attempted to execute the warrant but was unable to access the device because it was protected by a passcode that the DEA could not bypass. *See* DE 19 (transcript of hearing dated Oct. 26, 2015) ("Tr.") at 6-7. The government asserts that the DEA consulted with the FBI, which also claimed it was unable to bypass the passcode.[4] *See id.* There is no evidence in the record that the government consulted with any other governmental entities or third parties. *See infra* III.D.1. In fact, the government refused to make the representation that it had engaged in such consultations when asked by Judge Orenstein on the record, and later claimed it had no obligation to do so. *See* Tr. 34-35; DE 21 at 8.

C. The Government Seeks To Enlist Apple To Extract Data From Feng's iPhone.

Not until October 2015, nearly three months after the warrant issued and on the eve of Feng's trial, did the government approach Apple regarding execution of the warrant to search Feng's iPhone. In response to that inquiry, Apple informed the government that the contents of the phone were not backed up to Apple's iCloud storage service and that the phone had a remote

[4] The record does not establish whether the government attempted to access certain types of data (*i.e.*, a log of recent telephone calls) that, depending on user settings, may be accessible without entering the passcode. DE 29 at 4 n.4.

wipe request pending. *See* DE 15 at 8. Apple later informed the government that the remote wipe request would not function on Feng's iPhone. *See* Tr. 32-33.

On October 8, 2015, the government applied to Judge Orenstein, serving as duty magistrate, for an *ex parte* order compelling Apple to bypass the security passcode on Feng's iPhone. DE 1 (the "Initial Application"). The Initial Application cited the All Writs Act, 28 U.S.C. § 1651, as the basis for the Court's authority to issue such an order. DE 1 at 2. The government submitted with its Initial Application a proposed order. *See id.*; DE 1-1. The proposed order included certain language from Apple's law enforcement compliance manual outlining how Apple would obtain the data it was being ordered to produce. Apple included this language in its manual in response to the government's prior reliance on orders that failed to specify the scope of Apple's obligations and did not correspond to the procedures that Apple had available to perform extractions and deliver data to law enforcement. To make clear what Apple could and could not do, Apple opted to include in its law enforcement manual proposed language specifying what it would do when ordered to perform extractions. Nowhere in that manual, however, does Apple concede that the All Writs Act is a proper basis to compel Apple to perform data extractions.[5]

On October 9, 2015, Judge Orenstein issued a memorandum and order deferring decision on the government's Initial Application and observing that whether the All Writs Act was properly invoked depended on "whether the government seeks to fill in a statutory gap that

[5] The government asserts in its application to this Court that "Apple has developed guidance for law enforcement agents for obtaining lawful court orders to request such a bypass." DE 30 at 5. As Judge Orenstein observed in response to the same representation, this "could be read to suggest that Apple somehow proposed or approved the government's reliance on the AWA as authority for the request." DE 29 at 4 n.4. That is not the case. As Judge Orenstein noted in rejecting such a suggestion, "it is only the [Initial] Application itself that cites the AWA; the proposed order submitted with it does not, but instead contains the technical language specifically describing the assistance the government wants Apple to provide." *Id.*

Congress has failed to consider, or instead seeks to have the court give it authority that Congress chose not to confer." DE 2 at 2. Analyzing the All Writs Act, relevant case law, and pertinent legislative enactments, Judge Orenstein "conclude[d] that the authorities on which the government relies do not support the conclusion that the All Writs Act permits the relief the government seeks." *Id.* at 10. Judge Orenstein nevertheless directed Apple to submit its views on whether compliance with the government's application would be technically feasible, and if so, whether compliance would be unduly burdensome. *Id.* at 1.

On October 19, 2015, Apple responded to the Court's memorandum and order, providing relevant technical information regarding the security features of iOS devices and explaining that for the dwindling number of Apple devices running iOS 7, Apple has the technical ability to extract certain categories of unencrypted data from a passcode-locked device. DE 11 at 2-3. Apple also identified the burdens that complying with the government's application would impose on Apple. *Id.* at 3-4. The government replied to Apple's opposition on October 22, 2015, DE 15, and at the Court's direction, Apple submitted a supplemental brief a day later, addressing the applicability of the All Writs Act to the order the government sought, DE 16.

On October 26, 2015, the Court heard oral argument. DE 18. At the outset, Judge Orenstein brought to the parties' attention certain materials from *United States v. Djibo*, No. 15-CR-88 (SJ) (E.D.N.Y.), an unrelated criminal matter. *See* Tr. 3. In particular, Judge Orenstein provided the parties with a letter submitted by the Department of Justice in *Djibo*, in which it represented that Homeland Security Investigations ("HSI") "is in possession of technology that would allow its forensic technicians to override the passcode security feature on the Subject

iPhone and obtain the data contained therein."[6] *See* Ex. J [*Djibo*, No. 15-CR-88 (SJ), DE 27 (E.D.N.Y. July 9, 2015)]. Judge Orenstein also provided the parties with a transcript from a hearing held on the defendant's motion to suppress in *Djibo* that contained testimony from an FBI Special Agent asserting that he had personally bypassed an iPhone running a version of iOS 7, the same operating system at issue here. *See* Ex. K [*Djibo*, No. 15-CR-88 (SJ), DE 65, 9/3/15 Hearing Transcript, at 17; 29-31 (E.D.N.Y. Oct. 16, 2015)].

Judge Orenstein also asked the government at the hearing whether it could represent that it sought assistance from other government agencies outside the FBI and DEA, including the intelligence community, to bypass the passcode of the device. *See* Tr. 34. The government would only represent that "the FBI and DEA do not have a reasonable [sic] available tool." *Id.* at 34-35. Nor did the government make the requested representation in its post-hearing submission, arguing instead that criminal prosecutors are not "required to consult with intelligence agencies or with other components that are not part of the prosecution team before applying for relief under the All Writs Act." DE 21 at 8. All told, the government offered no evidence that it had consulted with any other agencies or third parties to determine that Apple's assistance was actually necessary, or that it had exhausted other potential repositories of the information it seeks to extract from Feng's iPhone, such as Feng himself, cell-phone service providers, email providers or social media services.

Nor did the government exhaust traditional investigative tools that were suggested to the government by Apple. In fact, the government issued Apple a single subpoena in this case,

---

[6] In *Djibo*, the defendant argued that evidence seized from his iPhone should be suppressed because he was asked for, and he provided, the passcode to the phone without being advised of his Miranda rights. *United States v. Djibo*, 2015 WL 9274916, at *2 (E.D.N.Y. Dec. 16, 2015). One of the bases on which the government opposed defendant's motion was that the records he sought to suppress would have been discovered using the passcode bypass technology that HSI possessed. *Id.* at *5.

seeking device connection and Internet Protocol address logs for Feng's iPhone, which Apple provided. The government never sought orders to obtain a log of the remote wipe request on Feng's iPhone or to obtain other potentially useful information pursuant to 18 U.S.C. § 2703(d).

D. Following Mr. Feng's Guilty Plea, The Government Continues Its Efforts To Compel Apple To Extract Data From His iPhone.

On October 29, 2015, without the government or Apple having extracted any information from Feng's iPhone, Feng pled guilty to conspiracy to distribute and possess with intent to distribute methamphetamine. *Yang*, 14-CR-387 (MKB), DE 119.

A day later, in response to a notification from the government that the defendant had pled guilty, Judge Orenstein ordered the government to explain why its application was not mooted by Feng's plea. *See* DE 25. The government responded the same day, asserting for the first time that investigation into the drug-trafficking conspiracy involving Feng was ongoing. *Id.* The government's letter also noted that Feng's case remains open until his sentencing, *see id.*, although it did not explain how any information potentially stored on his iPhone might alter the advisory sentencing guidelines range that would apply to him. *See* DE 29 at 6.

The government took no further action on its application for over three months.[7]

[7] In the interim, Apple continued to receive additional demands from the government to extract unencrypted data from a variety of iOS devices in different jurisdictions, all of which invoked the All Writs Act as the basis for courts' authority to issue such orders. *See* DE 27 at 2. Apple objected to performing extraction services on those devices. DE 27 at 2-3. In the recent San Bernardino Matter, the government claimed that the All Writs Act provided authority for the government to compel Apple to create a new operating system to disable security measures on an iOS 9 device. *See* Ex. L [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 1 at 14 (C.D. Cal. Feb. 19, 2016)]. The government subsequently abandoned that demand. While Apple agrees with the government that the San Bernardino Matter is factually distinct, its belated admission that Apple's assistance was not necessary to unlock the iPhone there, at the very least, calls into question the credibility of its contention—wholly unsupported by any evidence in the record—that Apple's assistance is necessary in this case. *See* Ex. C [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 209 (C.D. Cal. Mar. 28, 2016)]; *see also infra* III.D.1.

E. Judge Orenstein's Opinion.

On February 29, 2016, in a 50-page order, Judge Orenstein recognized that the All Writs Act cannot be used to compel Apple to perform expert forensic services for the government and denied the government's Initial Application. DE 29.

First, Judge Orenstein concluded that, although the relief sought by the government would be in aid of the Court's jurisdiction, *see* DE 29 at 12-13, and "necessary or appropriate" in light of both the Act's language and relevant case law construing it, *see id.* at 13, the government failed to satisfy the All Writs Act's requirement that the requested relief be "agreeable to the usages and principles of law." *See id.* at 14-30. Adhering to a longstanding canon of statutory construction, Judge Orenstein gave meaning to each word of the clause "agreeable to the usages and principles of law," and concluded that an order issued under the authority of the All Writs Act must comport with other relevant statutes and prior congressional action. *Id.* at 21-24. In doing so, he rejected the government's contention, repeated here, that the phrase "agreeable to the usages and principles of law" empowers the judiciary to issue any order not explicitly prohibited by another Congressional statute. *Id.*

Second, Judge Orenstein analyzed the effect of CALEA on the Court's power to compel Apple, as the creator of Feng's iPhone and iOS 7, to assist the government in bypassing its security features and extracting its encrypted data. DE 29 at 16-21. CALEA imposes certain obligations on "telecommunications carriers" to ensure that their equipment and services permit the government to intercept a subscriber's communications pursuant to a court order. *Id.* at 20. But for entities that are "information services" providers, as defined under CALEA, or that fall outside of CALEA's ambit, Judge Orenstein concluded that the absence of statutory requirements to aid law enforcement reflects a deliberate omission by Congress. *Id.* at 19-20. Judge Orenstein rejected as a violation of separation of powers the government's interpretation

that Congress, by specifically protecting "telecommunications carriers" from a requirement to build an encryption backdoor into their products, otherwise declared open season under the All Writs Act on any entity that did not qualify as a telecommunications carrier. *Id.* at 25-26. Accordingly, he held that the executive branch could not use the All Writs Act to expand the government's ability to compel third party assistance with electronic surveillance further than Congress had authorized. *Id.* at 16-20.

Third, Judge Orenstein concluded that even if the All Writs Act permitted the government's request, that request was nonetheless unlawful under the Supreme Court's decision in *New York Telephone*. *See* DE 29 at 31. In particular, Judge Orenstein analyzed Apple's connection to the underlying criminal investigation and concluded that Apple did not facilitate or participate in Mr. Feng's criminal activity by selling him an iPhone, *id.* at 31-33, had done nothing to thwart the government's investigation, *id.* at 35, and was not closely related to the investigation as a result of its practice of licensing its iOS operating system to its users, *id.* at 32. Judge Orenstein further concluded that the government's request would pose an undue burden on Apple, *id.* at 43-44, and that the government had failed to establish that Apple's assistance was necessary because different government entities had made conflicting statements in this and other proceedings that cast doubt on whether the government actually required Apple's assistance to access Feng's iPhone. *Id.* at 45-48.

F. The Government's Application To This Court.

On March 7, 2016, the government filed a brief before this Court, styled as a resubmission of its application, seeking to replace Judge Orenstein's order. DE 30. The government's application to this Court seeks the same relief that Judge Orenstein denied under the All Writs Act. DE 30-1 (the "March 7 Application"). As support for the March 7 Application, the government reattached the July 6, 2015 Affidavit of Special Agent Benjamin X.

Yu in Support of Application for a Search Warrant, in which Special Agent Yu identified the information he hoped to obtain from Feng's iPhone, including "records of communications such as call logs, chats, and text messages" and "things that have been viewed via the Internet." DE 30-3 ¶¶ 24-25. On April 8, 2016—notwithstanding that the government withdrew its application in the San Bernardino Matter because, contrary to the government's prior assertions, Apple's assistance was unnecessary in that case—the government submitted a letter to this Court stating that it would not modify its application. DE 39.

III. ARGUMENT

A. Judge Orenstein's Order Should Be Reviewed Under The "Clearly Erroneous or Contrary to Law" Standard.

In its papers, the government takes great pains to characterize its brief as a *renewed* application rather than an appeal from Judge Orenstein's order, presumably to bolster its contention that Judge Orenstein's order should be reviewed *de novo*. *See* DE 30 at 12.[8] In doing so, the government attempts to obscure the fact that this matter was extensively briefed, a hearing was held, supplemental briefing was provided, and Judge Orenstein issued a 50-page order. Moreover, the government's insistence that it is entitled to a do-over is belied by Federal Rule of Criminal Procedure 59 and Section 636 of the Federal Magistrates Act.

Federal Rule of Criminal Procedure 59 prescribes the standards of review to be applied by a district court when considering a challenge to a magistrate judge's order. Rule 59 distinguishes between "dispositive" orders, which include a "motion to dismiss or quash an indictment or information, a motion to suppress evidence, or any matter that may dispose of a charge or defense," and "nondispositive" orders, which encompass "any matter that does not

[8] On the docket for the proceedings before Judge Orenstein, however, the government described its application as an "Appeal of Magistrate Judge Decision to [the] District Court." DE 30.

dispose of a charge or defense," Fed. R. Crim. P. 59(a)-(b).[9] While *de novo* review is reserved for objections to dispositive orders, nondispositive orders must be reviewed under the "contrary to law or clearly erroneous" standard. *Compare* Fed. R. Crim. P. 59(b)(3), *with* Fed. R. Crim. P. 59(a). These standards apply regardless whether the magistrate judge is acting pursuant to § 636(b)(1) of the Federal Magistrates Act or § 636(b)(3), as the government suggests here. *See United States v. Warshay*, 1998 WL 767138, at *3 (E.D.N.Y. Aug. 4, 1998) ("[Alt]hough § 636(b)(3) prescribes no review procedures, courts have borrowed both the dispositive-nondispositive distinction and the review procedures of subsection (b)(1)."); *see also United States v. Premises Known as 281 Syosset Woodbury Rd.*, 862 F. Supp. 847, 851 (E.D.N.Y. 1994), *aff'd*, 71 F.3d 1067 (2d Cir. 1995).

The government's search warrant for the devices recovered from Feng's residence and its subsequent application to compel Apple to bypass the security features on his phone were brought in furtherance of an ongoing criminal case against him, DE 30 at 12, and thus did not dispose of any "charge or defense" in that proceeding. In fact, no charges were disposed of until October 2015 when Mr. Feng pled guilty, while the government's application was pending. *See Yang*, 14-CR-387 (MKB), DE 119. Because the application and Judge Orenstein's order did not dispose of any charge or defense, the order's factual determinations must be reviewed for clear error. *See, e.g.*, *Matter the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157, 162 (D.D.C. 2014) (reviewing for

[9] Section 636(b)(1) of the Federal Magistrates Act also distinguishes between dispositive matters ("a motion for injunctive relief, for judgment on the pleadings, for summary judgment, to dismiss or quash an indictment or information . . . to dismiss for failure to state a claim upon which relief can be granted, and to involuntarily dismiss an action," 28 U.S.C. § 636(b)(1)(A) and nondispositive "pretrial matter[s]," *id.* § 636(b)(1). Consistent with Rule 59, nondispositive pretrial matters may be reconsidered only "where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law." *Id.* § 636(b)(1)(A).

clear error); *In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 2006 WL 2871743, at *1 (E.D. Wis. Oct. 6, 2006) (same); *see also New York v. Mountain Tobacco Co.*, 953 F. Supp. 2d 385, 389 (E.D.N.Y. 2013); E.D.N.Y. Loc. Crim. R. 59.1(c) (applying E.D.N.Y. Local Civil Rule 72.1 in criminal proceedings).[10]

B. The All Writs Act Does Not Authorize The Order The Government Seeks Here.

The government contends that the All Writs Act should be broadly construed to "permi[t] 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.'" DE 30 at 14 (quoting *N.Y. Tel.*, 434 U.S. at 172-73). One struggles to find any limiting principle in that account of the Act's scope. But the government goes even further, urging the Court to wield this power "flexibly." *Id.* Applying its boundless construction of the All Writs Act to this case, the government asserts that courts have authority to issue ancillary orders to third parties to facilitate the execution of search warrants, subject only to two limitations: (1) that the order does not impose an "unreasonable burden" (*id.*

[10] Two of the cases cited by the government for the proposition that *de novo* review applies contain no analysis of the proper standard of review and do not cite to Rule 59 or § 636. *See In re Application of the U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Tel.* ("*Certain Cellular Telephone*"), 460 F. Supp. 2d 448, 454 (S.D.N.Y. 2006); *see also In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information* ("*Historical Cell Information*"), 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011). And while the third case states that cases decided under § 636(b)(3) are subject to *de novo* review, it does so without acknowledging the distinction between dispositive and nondispositive matters, and wholly ignores authority holding that this distinction applies even when a case is brought under § 636(b)(3). *See In re Application of the U.S. for an Order of Nondisclosure* ("*Order of Nondisclosure*"), 41 F. Supp. 3d 1, 3 (D.D.C. 2014); *cf. Warshay*, 1998 WL 767138, at *3. Moreover, each of these cases involved requests for a warrant *prior to the charging of any criminal defendant*. Accordingly, unlike this case, there was no underlying criminal case subject to the ongoing supervision and control of a district judge, *cf.* DE 30 at 12 ("This Court retains . . . 'supervision and control' of matters delegated to magistrate judges in connection with the Feng investigation."), meaning that the magistrate judge's opinion was the final disposition of the legal action concerning the investigation, *see Order of Nondisclosure*, 41 F. Supp. at 3 (concerning grand jury subpoena); *Historical Cell Information*, 809 F. Supp. 2d at 114 (concerning cell-site location records); *Certain Cellular Telephone*, 460 F. Supp. 2d at 448 (seeking prospective cell-site location data).

at 15), and (2) that Congress has not "express[ly] or implied[ly] prohibit[ed] the requested relief" (*id.* at 26). In the government's account, however, these are no limitations at all. Congress simply cannot be expected to preemptively prohibit every overreaching order the government might dream up in furtherance of a valid warrant. The Court should reject the government's interpretation of the Act as inconsistent with the statute's text, history, and relevant precedent. By its terms, the All Writs Act authorizes federal courts to 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 Act's reference to "writs" "agreeable to the usages and principles of law" is understood to refer to "traditional writs that have not been altered or abolished by some other statute." *Lowery v. McCaughtry*, 954 F.2d 422, 423 (7th Cir. 1992). Underscoring the Act's close connection to the common law, the Act specifically referenced two of the most well-known common law writs, *habeas corpus* and *scire facias*. *See* An Act to Establish the Judicial Courts of the United States, § 14, 1 Stat. 81 (1789). The Act thus grants federal courts power to issue the established common law writs in use at the time of the American Founding, such as, *inter alia*, *certiorari*, *mandamus*, *quo warranto*, and *capias*. *See* Edward Jenks, *The Prerogative Writs in English Law*, 32 Yale L.J. 523, 527-34 (1923); F.W. Maitland, *The History of the Register of Original Writs*, 3 Harv. L. Rev. 97 (1889) (describing the "*Registran Brevium*—the register of writs current in the English Chancery"). Accordingly, "[i]n determining what auxiliary writs are 'agreeable to the usages and principles of law,' [the Court] look[s] first to the common law." *United States v. Hayman*, 342 U.S. 205, 221 n.35 (1952). Indeed, the government concedes the phrase "agreeable to the usages and principles of law" "refers to the collection of historical writs that formed the basis of English and early

American legal systems." DE 30 at 29 (citing *Bank of U.S. v. Halstead*, 23 U.S. (10 Wheat.) 51 (1825)).

Because the Act is grounded in the common law, it cannot be construed as a "grant of plenary power to the federal courts" or to "give the district court a roving commission" to order private parties to assist the government. *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). Rather, as Judge Orenstein recognized, it "function[s] as a 'gap filler,'" DE 29 at 14, that "suppl[ies] the courts with the instruments needed to perform their duty," *Harris v. Nelson*, 394 U.S. 286, 300 (1969); *see also Trenkler v. United States*, 536 F.3d 85, 97 (1st Cir. 2008). For example, Congress has authorized courts to issue "the writ of *habeas corpus ad testificandum*," such that a "court may direct the custodian to produce the prisoner in court as a witness." *Ivey v. Harney*, 47 F.3d 181, 183 (7th Cir. 1995). But "[w]at happens if the testimony takes two days? Where does the prisoner stay overnight? . . . The statute does not say; neither, however, does it subtract from the court's common law powers to control such details." *Id.* In this instance, the All Writs Act would fill the gap as a "residual source of authority" empowering the court "to issue writs that are not otherwise covered by [the] statute." *Clinton v. Goldsmith*, 526 U.S. 529, 537 (1999) (internal quotation marks omitted).

The order the government seeks here, which would require Apple to take possession of and use its own technology to extract data from a device over which it has no custody or control, is neither grounded in the common law nor authorized by statute. *See infra* III.C. The government suggests that Apple conceded before Judge Orenstein that the order sought here has "'a close enough antecedent in the common law,'" DE 30 at 30 (quoting DE 29 at 14 n.10), but Apple made no such concession. On the contrary, Apple consistently argued that the All Writs Act does not authorize the requested order. DE 16 at 4-8. The government is thus incorrect

when it insists that there is "no dispute between the parties that the writ sought herein" is "agreeable to the usages and principles of law . . . ." DE 30 at 30.

The government is also incorrect when it contends that *Halstead* "fatally undermines" Judge Orenstein's interpretation of the All Writs Act. DE 30 at 31. The "principal inquiry" in that case was "whether the laws of the United States authorize the Courts . . . to alter the form of the process of execution, which was in use in the Supreme Courts of the several States in the year 1789, [so] as to uphold the *venditioni exponas* issued in this cause." *Halstead*, 23 U.S. (10 Wheat.) at 54-55.[11] The question arose because the Process Act of 1792 provided that "the forms of writs and executions, and modes of process, in the Circuit and District Courts, in suits at common law, shall be the same in each State respectively, as are *now* used or allowed in the Supreme Courts of the same," *id.* at 57, *and* that this limitation was "subject . . . to such alterations and additions, as the said Courts respectively shall, in their discretion, deem expedient" *id.* at 58. Interpreting these provisions, the Court explained that federal courts "have authority . . . from time to time to alter the process, in such manner as they shall deem expedient, and likewise to make *additions* thereto, which necessarily implies a power to enlarge the effect and operation of the process." *Id.* at 60. The Court rejected the argument that modifying the forms of the writ and the modes of process was an improper "exercise of legislative power," because the limited "power given to the Courts over their process is no more than authorizing them to regulate and direct the conduct of the Marshal, in the execution of the process." *Id.* at 61. The narrow holding of *Halstead* was thus that the "operation of an execution" was not

[11] A writ of execution is a common law writ that a court issues directing a law enforcement officer to sell property in satisfaction of a judgment. *See Halstead*, 23 U.S. (10 Wheat.) at 55 ("That executions are among the writs hereby authorized to be issued, cannot admit of a doubt . . . ."); *Wayman v. Southard*, 23 U.S. 1, 22 (1825) ("An execution is a writ, which is certainly 'agreeable to the principles and usages of law.'").

limited "to that which it would have had in the year 1789[.]" *Id.* at 62; *cf. Beers v. Haughton*, 34 U.S. (9 Pet.) 329, 360 (1835) (explaining that the practical result in *Halstead* was that a writ of execution "may reach property not liable, in 1789, by the state laws to be taken in execution, or may exempt property, which was not then exempted, but has been exempted by subsequent state laws").

The authority to alter the *forms* and *process* of traditional common law writs is not authority to invent new writs with no common law analogue. But that is precisely what the government is asking the Court to do here—to issue an order with no common law analogue, directing an unrelated third party to use its own technological know-how to extract data from a device in the government's possession. *Cf. Ivey*, 47 F.3d at 185 (reversing order issued under the All Writs Act because "[n]othing in the common law supports an order directing a third party to provide free services that facilitate litigation").[12] The Court should reject the government's "call[] for 'creative' use of federal judicial power" lacking any foundation in the common law. *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 40 (1985); *cf. Ivey*, 47 F.3d at 185 (considering "hypothetical parallel[s]" showing that petitioner's reading of the All Writs Act would allow the court to issue all sorts of orders not allowed at common law).

The government's legal authorities are not to the contrary, as they overwhelmingly involve All Writs Act orders addressed to third parties whose facilities were being used to

[12] In fact, the requested order is akin to an injunction directing specific performance of a personal services contract, a remedy the common law specifically disfavored. *See* Restatement (Second) of Contracts § 367 ("A promise to render personal service will not be specifically enforced"); *Virginian Ry. Co. v. Sys. Fed'n No. 40*, 300 U.S. 515, 550 (1937) ("Equity will not . . . compel one to enter into performance of a contract of personal service which it cannot adequately control.").

facilitate suspected ongoing criminal activity,[13] and where the information being sought was in the third parties' possession.[14] DE 30 at 16; *see infra* III.D.2. Unlike the order requested here, these writs fit squarely within the common law tradition. As the government notes, courts may issue orders to third parties outside of the law enforcement context where the plaintiff demonstrates that the defendant is using the third party's facilities to violate the plaintiff's rights. DE 30 at 16 n.3 (discussing All Writs Act orders to third parties to support injunctive relief). And there is nothing novel about requiring a third party to produce documents or records in its possession for use in a criminal case. *See, e.g.*, *United States v. Burr*, 25 F. Cas. 30, 30-37 (C.C.D. Va. 1807) (holding that subpoena *duces tecum* could be issued to President Jefferson directing him to produce, *inter alia*, a letter he received from General Wilkinson with potential relevance to Burr's criminal case). What courts have *not* historically had the authority to do is order a third party to use its proprietary technological know-how to help the government access information that is already in *the government's possession*.

To be sure, courts have previously issued *ex parte* orders directing Apple to "assist in extracting data from an Apple device through bypassing the passcode in order to execute a

---

[13] *See 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) (suspects using company's phone lines in furtherance of criminal enterprise); *In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1123-24 (9th Cir. 1980) ("*Mountain Bell*") (same).

[14] *See United States v. Doe*, 537 F. Supp. 838, 839 (E.D.N.Y. 1982) (ordering phone company to produce toll records because they could "reveal the present whereabouts of the subscriber's daughter"); *United States v. X*, 601 F. Supp. 1039, 1040 (D. Md. 1984) (ordering production of toll records believed to be "of critical importance in locating defendant X"); *United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (ordering credit card company to produce records of customer believed to be harboring a fugitive); *In re Application of U.S. for an Order Directing X to Provide Access to Videotapes* ("*Videotapes"*), 2003 WL 22053105, at *1, *3 (D. Md. Aug. 22, 2003) (ordering third party "merely to provide access to surveillance tapes already in existence, rather than any substantive assistance" so that the government could "locate defendant Y and . . . execute a warrant for [his/her] arrest").

search warrant." DE 30 at 17 (citing cases). But the government's cited orders were issued *ex parte*, without Apple's participation, without the benefit of adversarial briefing on the scope of the All Writs Act, and with no supporting analysis. Apple also was not a party in *United States v. Blake*, No. 13-CR-80054 (S.D. Fl. July 14, 2014), in which the court denied the defendant's motion to suppress evidence gathered from an iPhone that Apple helped unlock. Accordingly, such cases are not even persuasive authority on the scope of the All Writs Act, let alone precedential; certainly such *ex parte* orders issued with little analysis should carry less weight than Judge Orenstein's lengthy and reasoned opinion.[15]

Because the order the government seeks goes well beyond the common-law powers authorized by the All Writs Act, and the All Writs Act confers interstitial rather than plenary authority, the Court can only grant the government's requested relief if some other statute provides it with such authority. There is no such statute here. To the contrary, the relief the government seeks is inconsistent with existing statutory authority.

C. The Government's Request Is Inconsistent With CALEA And The Comprehensive Statutory Framework Of Which It Is A Part.

In attempting to expand the limited scope of the All Writs Act, the government seeks authority that Congress has expressly and impliedly rejected through CALEA, 47 U.S.C. § 1001 *et seq*., and the comprehensive legislative scheme of which CALEA is a part.

---

[15] The only court that did assess the scope of the All Writs Act in connection with a request to order a third party to unlock a cellular phone misread New York Telephone as standing for the proposition that a third party's assistance can be compelled whenever it has the ability to unlock a phone because its decision not to do so would "'frustrate'" the government's search efforts. *See In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant by Unlocking a Cellphone*, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014) (quoting *N.Y. Tel.*, 434 U.S. at 174). But if that were the rule, the government could conscript any third party with the ability to assist a search in any way on the ground on the ground that refusing to assist would "frustrate" law enforcement's efforts. That is not the law.

1. CALEA Specifically Exempts Information Service Providers From Having To Create Or Maintain Systems To Facilitate Government Access.

CALEA specifies the types of private companies that can be compelled to assist the government in accessing communications, the circumstances in which such assistance can be compelled, and the form that compulsory assistance may take—and it expressly excludes Apple, which serves as an "information services" provider, from being conscripted by law enforcement to provide it with access to stored communications. *See* 47 U.S.C. § 1001 *et seq*.

In drafting and enacting CALEA, Congress sought to ensure that "government surveillance authority is *clearly defined and appropriately limited*," H.R. Rep. No. 103-827(I), at 17 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3497 (emphasis added), and to "balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies," *id.* at 13, 1994 U.S.C.C.A.N. at 3493.

In keeping with these principles, CALEA requires "telecommunications carriers" to ensure that their "equipment, facilities, or services" enable the government to intercept communications pursuant to a court order or other lawful authorization. 47 U.S.C. § 1002. Expressly excluded from CALEA's definition of "telecommunications carrier" are persons or entities providing "information services," *id*. § 1001(8), a term CALEA defines to include "electronic messaging services" and services that "permit[] a customer to retrieve stored information from, or file information for storage in, information storage facilities," *id.* § 1001(6)(B)(i), (iii). CALEA thus reflects Congress's deliberate decision to exclude services that facilitate "information storage" from being forced to assist in government surveillance or accessing electronic information.

As relevant to the government's request in this case, Apple is an information services provider. In particular, FaceTime, iMessage, and Mail are all features of iOS 7 that serve as electronic messaging services that permit users to communicate and store passcode-protected electronic communications. *See* DE 29 at 20 (Judge Orenstein observing that "information services" provider is broadly defined in CALEA and "easily encompasses Apple"). The government attempts to avoid this reality by insisting that Apple should not be considered an "information services" provider for purposes of this case because Apple's only relevant role is as the "manufacturer of a consumer device." DE 30 at 19-21. But the government's position is inconsistent with its own admission that the requested order is intended to facilitate "access to [the device's] *contents*," *id.* at 4 (emphasis added), which the government expressly describes as "records of communications such as call logs, chats and text messages" and "things that have been viewed via the Internet," DE 30-3 ¶¶ 24-25; *see also* DE 30 at 34 (asserting the defendant facilitated drug deals by using his phone to make calls, send text messages, and chat). In other words, what is at issue in this case is access to communications that were exchanged using messaging services and information storage that Apple provides to its users in its capacity as an information services provider.

Finally, while insisting that Apple is merely a "manufacturer" for purposes of its CALEA analysis, *see* DE 30 at 20, the government relies on the very features that make Apple an information services provider to argue that Apple is not "too far removed" from this case in its *New York Telephone* analysis, *id*. at 34-35. The government cannot have it both ways. Because the assistance the government requests here implicates Apple's role as an information services provider, CALEA controls. Thus, Apple cannot be required to facilitate law enforcement access

to its information services—in real-time or after such communications are stored on a user's passcode-protected device. *See* 47 U.S.C. § 1001(6)(B)(i).

2. Congress's Comprehensive Statutory Scheme Addressing Third Party Assistance In Accessing Communications Delineates The Exclusive Means By Which Courts May Compel Such Assistance.

The government concedes that Congress can either "explicitly or implicitly" bar certain All Writs Act orders, DE 30 at 18, but nevertheless insists that its request in this case is permissible because there is no statute that *specifically* provides "procedures for requiring any device manufacturer, such as Apple, to extract data from a passcode-locked phone," *id.* at 19. It is difficult to reconcile the government's concession that Congress can "implicitly" bar certain All Writs Act orders with its insistence that Congress must speak with such specificity. Moreover, the government's demand for congressional precision in this case is at odds with the longstanding principle that statutes within a legislative scheme must be interpreted as part of "a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into [a] harmonious whole." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) (citations and internal quotation marks omitted).

Here, the "comprehensive legislative scheme" of which CALEA is a part specifically "prescribe[s] the extent to which law enforcement may secure access to a wide array of data—both 'in motion' and 'at rest'—[and imposes] obligations [on] some private entities but not others to provide affirmative assistance" to law enforcement. DE 29 at 20. In delineating the acceptability of certain government requests relating to surveillance and access to data, that scheme is "so comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the statute does not affirmatively prescribe." *Id.* at 15-16; *cf. Trenkler*, 536 F.3d at 97 ("[W]hen a statute . . . specifically addresses a particular *class of claims or issues*, it is that statute, not the All Writs Act, that takes precedence.") (emphasis added).

Thus, even if CALEA did not expressly bar the government from demanding Apple's assistance (and it does), the court is *impliedly* prohibited from compelling such assistance by the absence of any legal authorization in the comprehensive statutory scheme of which CALEA is a part.

The legislative scheme governing third party technical assistance for government surveillance and data collection efforts was developed over the course of decades and includes several congressional enactments, each of which identifies certain kinds of entities whose assistance can be compelled, the circumstances in which such assistance can be demanded, and the kind of assistance that can be required. *See* CALEA, 47 U.S.C. § 1002; Pen/Trap Statute, 18 U.S.C. § 3123(b)(2) (permitting the government to compel a third party to furnish "information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device"); Wiretap Act, 18 U.S.C. § 2518(4) (permitting the government to compel a third party to furnish "all information, facilities, and technical assistance necessary to accomplish the interception" of a "wire, oral, or electronic communication"); Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(2)(a)(ii) (amending the Wiretap Act to authorize "providers of wire or electronic communication service" "to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance"); Stored Communications Act ("SCA"), 18 U.S.C. § 2703(a) (providing that the government "may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant").[16]

[16] The parties agree that the ECPA, the SCA, the Wiretap Act, and the Pen/Trap Statute do not expressly cover the government's specific request in this case. *See* DE 30 at 22-23.

In addition to conferring certain, specific powers on law enforcement, these statutes include express limitations on compulsory third party assistance, thereby demonstrating Congress's deliberate effort to limit the scope of lawful third party conscription. CALEA, for example, explicitly *excludes* "information services" providers from its ambit, *see supra* III.C.1, while limiting what law enforcement can demand of both "telecommunications carriers" and "electronic communication service" providers.[17] Specifically, law enforcement cannot require "electronic communication service" providers to adopt "any specific design of equipment, facilities, services, features, or system configurations" to facilitate government access. 47 U.S.C. § 1002(b)(1)(A). Moreover, the SCA details when governmental entities can require providers of electronic communications and remote computing services to *produce* stored content to the government, but it does not obligate them to provide technical assistance. 18 U.S.C. § 2703(a), (b). Importantly, the SCA is limited to information held or maintained (in electronic storage, or otherwise) on the providers' systems and does not impose obligations on providers to assist the government in retrieving information stored on private computers or other devices. *Id.*

When viewed collectively, the requirements and limitations included in these statutes comprehensively specify the third parties from which the government can seek technical assistance and the kinds of assistance it can require. This framework is not, as the government contends, an "incomplete patchwork of statutes," DE 30 at 24; rather, as Judge Orenstein recognized, it is a highly complex legislative scheme in which both express provisions and omissions reflect Congress's reasoned compromise between the competing interests of third parties and law enforcement, DE 29 at 20. These deliberate policy choices, and the careful

[17] The term "electronic communication service" is broadly defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 47 U.S.C. § 1001(1); 18 U.S.C. § 2510(15).

balance struck by Congress, cannot be swept aside simply because the government finds it more convenient. *Cf. Pa. Bureau of Corr.*, 474 U.S. at 43 (the All Writs Act does not empower federal courts "to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate").

The government fails to grasp the scope and import of this statutory framework, insisting that CALEA is merely "tangential," DE 30 at 25, and likening the legislative scheme at issue here to the one in *New York Telephone*, in which the Supreme Court compelled a public telephone company to assist in setting up a pen register to intercept communications prior to Congress's enactment of the Pen Register statute, *id.* at 25-26. There, the Court reasoned that because the Wiretap Act required third party assistance in intercepting wire communications, "it would be remarkable if Congress thought it beyond the power of the federal court to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy." *N.Y. Tel.*, 434 U.S. at 176-77. Because the order was "consistent with the intent of Congress," the Court did not need to wait for Congress to "fill in" a gap when requiring third parties to assist in setting up lawful pen traps. *Id.* at 172. Here, by contrast, the government is not asking the Court to "fill in" a statutory gap through an order that is less invasive than those explicitly authorized; it is asking the Court to circumvent CALEA's express limitations and go beyond any statutory authorization currently on the books. Thus, unlike the order in *New York Telephone*, the government's demand here is demonstrably *inconsistent* "with the intent of Congress." *Id.*[18]

[18] Moreover, to the extent this area of law may have been a "patchwork" of statutes at the time *New York Telephone* was decided, it has since been expanded into a comprehensive scheme, and Congress continues to legislate actively in this area. *See* Pen/Trap Statute, Pub. L. No. 99-508, 100 Stat. 1848, 1869-70 (1986) (enacting 18 U.S.C. § 3123(b)(2)); Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783, 1796-97 (1978) (adding third party

The government nonetheless insists that the statutory scheme in this case is not sufficiently comprehensive, but its only support for this assertion is a collection of inapposite preemption cases. DE 30 at 25 (citing *Gonzalez v. Raich*, 545 U.S. 1, 10, 15 (2005) (describing the detailed federal scheme regulating marijuana in the context of assessing Congress's Commerce Clause powers); *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 351 (1984) (concluding that because Congress's intent to preclude judicial review of agency action was "fairly discernible" from the detail of a legislative scheme, it overcame a contrary presumption); *Arizona v. United States*, 132 S. Ct. 2492, 2500-01 (2012) (explaining that, under the Supremacy Clause and federalism principles, the field preemption doctrine applies to "a field in which Congress has left no room for States to regulate").

The government characterizes the limits on courts' authority to issue orders under the All Writs Act—including orders directing a third party to unlock a phone in the government's possession—as exceedingly narrow, contending that any order is permissible so long as "that specific relief" has not been "explicitly or implicitly prohibited by law." DE 30 at 18. But the cases the government cites—*Pennsylvania Bureau of Correction*, *New York Telephone*, and *United States v. Barret*, 178 F.3d 34 (1st Cir. 1999), *id.*, say no such thing. Rather, those cases stand only for the unremarkable proposition that an otherwise lawful writ may not be issued where Congress has affirmatively prohibited it. *Cf. Trenkler*, 536 F.3d at 97 "[W]hen a statute . . . specifically addresses a particular class of claims or issues, it is that statute, not the All Writs Act, that takes precedence."). None of the government's cases (or any other case) holds that the All Writs Act gives courts *carte blanche* to issue any order the government might request when

---

language to 18 U.S.C. § 2511(2)(a)(ii)); ECPA, Pub. L. No. 99-508, 100 Stat. at 1849-51 (amending same); SCA, Pub. L. No. 99-508, 100 Stat. at 1861 (enacting 18 U.S.C. § 2703); USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 274, 283 (2009) (amending same).

Congress has remained silent (which, in any event, is not the case here). On the contrary, in the face of congressional silence, the court must "look . . . to the common law" to determine whether a writ is "agreeable to the principles and usages of law." *Hayman*, 342 U.S. at 221 n.35. As previously discussed, *see supra* III.B, the type of writ the government seeks here is wholly foreign to the common law and is therefore unavailable under the All Writs Act.

3. Use Of The All Writs Act Would Usurp Congressional Authority.

Congress has continued to consider the scope of permissible government impositions on third parties, and the Court should not allow the All Writs Act to be used to invade the province of the legislature. The Supreme Court in *New York Telephone* recognized the role of congressional intent in its All Writs Act analysis, relying on the fact that its order was "consistent with the intent of Congress" and with "recent congressional actions." 434 U.S. at 172, 176. Here, Congress has considered but declined to enact legislation to provide the government the very authority it seeks in these proceedings. This silence, when viewed in the context of the existing statutory scheme regarding electronic surveillance and third party assistance to law enforcement in accessing communications, is not meaningless or indicative of a "gap" to be filled by the All Writs Act. Rather, it reflects a deliberate legislative decision reflecting Congress's carefully calibrated balance of third party and law enforcement interests.

The government wrongly asserts that legislative intent can never be discerned from an absence of affirmative legislation. *See* DE 30 at 26-27. While silence can be a weak indicator of congressional intent in some circumstances, it is a different story altogether when Congress actively considers legislation to address a major policy issue but deliberately declines to enact it.

Here, Congress opted to require certain third party assistance through several different enactments designed to aid law enforcement in gathering electronic evidence (although none as expansive as what the government seeks here), but it has declined to include similar provisions in

other statutes, despite vigorous lobbying by law enforcement and notwithstanding its "prolonged and acute awareness of so important an issue" as the one presented here. *Bob Jones Univ. v. United States*, 461 U.S. 574, 601 (1983). Accordingly, the lack of statutory authorization in CALEA or any of the complementary statutes in the "comprehensive federal scheme" of surveillance and telecommunications law speaks volumes. *P.R. Dep't of Consumer Affairs v. Isla Petrol. Corp*., 485 U.S. 495, 503 (1988) ("Where a comprehensive federal scheme intentionally leaves a portion of the regulated field without controls, *then* the preemptive inference can be drawn—not from federal inaction alone, but from inaction joined with action.").

That the Executive Branch recently abandoned plans to seek legislation expanding CALEA's reach provides additional confirmation that Congress has not acceded to the government's wishes, and belies the government's view that courts have possessed authority to issues these types of orders under the All Writs Act since 1789.[19] Although the Administration is free to keep its powder dry for future lobbying efforts, it cannot use the courts to rewrite federal legislation or circumvent legislative intent. As explained above, CALEA prohibits compelling Apple to assist the government in the manner it seeks here, and this Court should decline the government's invitation to violate the separation of powers by usurping Congress's

[19] Federal officials familiar with that failed lobbying effort confirmed that the FBI had in fact developed a "draft proposal" containing a web of detailed provisions, including specific fines and compliance timelines, and had floated that proposal with the White House. *See* Ex. M [Ellen Nakashima, *Proposal Seeks To Fine Tech Companies for Noncompliance with Wiretap Orders*, Wash. Post (Apr. 28, 2013)]. As *The Washington Post* reported, advocates of the proposal within the government dropped the effort, because they determined they could not get what they wanted from Congress at that time: "Although 'the legislative environment is very hostile today,' the intelligence community's top lawyer, Robert S. Litt, said to colleagues in an August [2015] e-mail, which was obtained by The Post, 'it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement.' There is value, he said, in 'keeping our options open for such a situation.'" Ex. N [Ellen Nakashima & Andrea Peterson, *Obama Faces Growing Momentum to Support Widespread Encryption*, Wash. Post (Sept. 16, 2015)].

"exclusive constitutional authority to make laws." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 588-89 (1952); *see* DE 29 at 12.[20]

The government's reliance on *FTC v. Dean Foods Co.*, 384 U.S. 597 (1966), DE 30 at 28-29, is misguided, as that case concerned the powers of the Federal Trade Commission, not the powers of courts under the All Writs Act, 384 U.S. at 609. Similarly inapposite are *United States v. Craft*, 535 U.S. 274 (2002), and *Zino Davidoff SA v. CVS Corp.* 571 F.3d 238 (2d Cir. 2009), which the government invokes for the unremarkable proposition that, oftentimes, several different equally tenable conclusions can be drawn from failed legislation, including that Congress thought existing legislation already encompassed the proposed enactment.[21] *See Craft*, 535 U.S. at 287; *Zino*, 571 F.3d at 243 (explaining that a failed attempt to amend the Lanham Act "to state a proposition with unmistakable clarity tells nothing about whether the preexisting [trademark] law already covered the point, albeit less clearly"). Such an inference is not tenable here, where Congress has faced sustained lobbying efforts, opted to provide and withhold authorizations in a "comprehensive federal scheme" of surveillance and telecommunications

[20] The government relies on several inapposite cases to argue that failed legislation universally lacks significance. *See* DE 30 at 27-28 (citing *INS v. Chadha*, 462 U.S. 919 (1983) (stating the uncontroversial proposition that laws cannot be passed without bicameralism and presentment, without discussing the import of legislative silence for interpreting congressional intent); *United States v. Estate of Romani*, 523 U.S. 517, 535 (1998) (Scalia, J., concurring) (criticizing the majority for analyzing the impact of rejected legislation); *Bowsher v. Synar*, 478 U.S. 714, 733-34 (1986) (holding that when Congress reserved to itself the ability to act without passing additional legislation, it unconstitutionally impinged on the role of the executive)).

[21] The same is true of *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), which the government cites to highlight the difficultly of discerning congressional intent from anything other than enacted law. DE 30 at 27-28. *Clapper* involved a failed amendment that would have expressly provided for judicial review, but the fact that the amendment failed to pass was not probative because the amendment "encompassed more than the issue of judicial review" and did not contemplate the particular circumstances in which judicial review was sought in that case. 785 F.3d at 807.

statutes, *Isla Petroleum*, 485 U.S. at 503, actively debated granting the requested powers, and made an affirmative decision not to do so, *see Bob Jones*, 461 U.S. at 601.

D. The Government's Request Is Not Authorized By *New York Telephone*.

As Judge Orenstein observed, the government's request for assistance is based on a construction of the All Writs Act that would "upen[d] the separation of powers," DE 29 at 26, and "cast doubt on the [Act]'s constitutionality if adopted." *Id.* at 12. The Court can avoid that constitutional thicket by deciding this case on narrower grounds. *See, e.g.*, *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 184 (1999). Indeed, even assuming that the All Writs Act can be invoked here (and it cannot as a matter of law, *see supra* III.B & III.C), the relief the government seeks is foreclosed by *New York Telephone*.

In that case, the district court had issued an order requiring the telephone company to provide the government with use of an otherwise unused telephone line so that the government could install a pen register on two lines that "had been, were currently being, and would continue to be used" in connection with an ongoing gambling enterprise. *N.Y. Tel.*, 434 U.S. at 162. The Supreme Court found the order authorized by the All Writs Act and "consistent with the intent of Congress." *Id.* at 172; *see also id*. at 176-77 (Congress "clearly intended" to provide for third party assistance with respect to pen registers, given statute providing for assistance with respect to Title III wiretaps).[22] Although the Court cautioned that "the power of federal courts to impose duties upon third parties is not without limits," *id.*, it upheld the district court's exercise of discretion for three reasons. *First*, the company's assistance was necessary, as without it "there [was] no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished." *Id.* at 175. *Second*, it observed that it "d[id] not think that the

[22] In contrast, as described *supra* III.B & III.C, the relevant statute, legislative history, and legislative scheme evince Congress's intent that the requested order *not* be available.

Company was a third party so far removed from the underlying controversy that its assistance could not be permissibly compelled," especially given that "the Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis." *Id.* at 174. *Third*, the Court ruled that the "order [was not] in any way burdensome" because the assistance sought was "meager" and the company was "a highly regulated public utility" for whom the use of pen registers was "by no means offensive to it." *Id.* at 174-75. In all of these respects, *New York Telephone* forecloses the government's request in this case.

1. The Government Has Utterly Failed To Demonstrate Necessity.

It is well established that a third party cannot be compelled to assist the government unless it demonstrates that the third party's participation is essential. *See N.Y. Tel.*, 434 U.S. at 164 n.5; *see also Plum Creek*, 608 F.2d at 1289-90 (denying All Writs Act application because "there has been no showing that the object to be achieved could not have been accomplished by using non-company employees"). In *New York Telephone*, the Court issued the order authorizing installation of a pen register only after observing that the FBI had conducted "an exhaustive search" and "was unable to find a location where it could install its own pen registers without tipping off the targets of the investigation." 434 U.S. at 175. Accordingly, the telephone company's participation was "essential to the fulfillment of the purpose" of the warrant—"there [was] *no conceivable way*" to install the pen register in an undetectable location without the company's assistance. *Id.* (emphasis added); *see also Mountain Bell*, 616 F.2d at 1129 (compelling third party to assist with tracing was necessary to carry out a wiretap—otherwise the tracing operation would be "completely frustrated"); *Mich. Bell Tel. Co. v. United States*, 565 F.2d 385, 389 (6th Cir. 1977) (telephone company was "the only entity that c[ould] effectuate the order . . . to prevent company-owned facilities from being used in violation of both state and federal laws").

Here, the government has failed to demonstrate that it has conducted an "exhaustive search" for alternative options to obtain the data from Feng's iPhone by any means other than compelling Apple to extract the data.[23] *First*, the government has not made any showing that it sought or received technical assistance from federal agencies with expertise in digital forensics. *See* Tr. 34-35. In fact, the government has failed to make any showing that it consulted non-intelligence agencies, and all but conceded to Judge Orenstein that it has not attempted to obtain such assistance from intelligence agencies, opting instead to insist that "federal prosecutors don't have an obligation to consult the intelligence community in order to investigate crime." Tr. 36.

Second, despite submitting a declaration in the San Bernardino Matter acknowledging that certain third parties have the ability to circumvent passcodes and other security mechanisms in different iPhone operating systems, *see* Ex. O [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 149-3, Decl. of Stacey Perino ¶ 28(a)-(e) (C.D. Cal. Mar. 10, 2016)], the government has made no showing that it has consulted any such third parties (or others) *in this case* and determined that Apple is the "only entity" that could "effectuate" the search warrant here. *See Mich. Bell*, 565 F.2d at 389. In its brief, the government asserts that it "has explored the possibility of using third party technologies but has determined that using such technology . . . presents the [] risk of triggering the auto-erase feature." DE 30 at 41. But it only describes communications with one government agent—who was brought to the government's attention by Judge Orenstein, Tr. 33—about one potential third party solution, *see* DE 30 at 43; *United States v. Djibo*, 2015 WL 9274916, at *6 (E.D.N.Y. Dec. 16, 2015) (discussing a tool that successfully

[23] While the government has argued in its briefing that it needs Apple's help, *see, e.g.*, DE 1 at 1; DE 15 at 20-21; DE 30 at 10, those statements are not evidence. And, to date, no one from the DEA, let alone a forensic agent, has corroborated those assertions via an affidavit, in stark contrast to the San Bernardino Matter, in which FBI agents submitted several declarations attesting to the need for Apple's assistance, even though those claims were later proven untrue.

bypassed the passcode on several iPhones). This is plainly inadequate—an exchange with a single third party is not an exhaustive search, and while the government may believe that compelling Apple to access Feng's iPhone is likely to be the most *efficient* or *cheapest* method of accessing the data, *see* DE 30 at 42, the All Writs Act "does not authorize a court to order a party . . . to aid the government in conducting a more efficient investigation, when other forms are available." *Plum Creek*, 608 F.2d at 1289-90 & n.5; *see also Bernstein v. Vill. of Piermont*, 2013 WL 5718450, at *4 (S.D.N.Y. Oct. 21, 2013) (denying All Writs Act relief because an "insurer's refusal to fund [a Village employee's defense] would not 'frustrate the implementation' of this Court's Order; it would merely mean that the Village must bear the cost directly"). Indeed, paying a third party other than Apple for the services the government wants Apple to perform is certainly a "conceivable way" to extract the data from Feng's iPhone without compelling Apple's involvement, as the government conceded by requesting vacatur of the order in the San Bernardino Matter.

Third, the government's claim of necessity is belied by its eleventh hour request to vacate its application in the San Bernardino Matter. *See* Ex. C [*In the Matter of the Search of an Apple iPhone*, No. 16-cm-10, DE 209 (C.D. Cal. Mar. 28, 2016)]; *see also supra* at 2. That the government submitted declarations in the San Bernardino Matter that it unequivocally needed Apple's assistance to access the iPhone in question—only to have those declarations later disproven when it acquired technology from a third party—shows that the government's knowledge of its own capabilities and those available in the marketplace was lacking, and thus its unsupported claims of necessity here are not credible. While the government has suggested publicly that the technology used in the San Bernardino Matter will not work on Feng's iPhone, it has made no showing that it has exhausted *other* methods in use by third parties that may be

able to access an iPhone 5s running iOS 7. *See, e.g.*, Ex. B [Kim Zetter, *How the Feds Could Get into iPhones Without Apple's Help*, Wired (Mar. 2, 2016)].[24] At the very least, in light of the successful assistance by a third party in the San Bernardino Matter, the government should have a heightened duty to make similar inquiries here before a last minute intervention results in further waste of judicial resources.

Fourth, the government has failed to show that it is has exhausted other potential repositories of the information it wants from Feng's iPhone. The government says that it seeks to learn Feng's customers and sources from the data on his iPhone, DE 30 at 8, but it has not shown, for example, whether it attempted to get this information by subpoenaing relevant records from Feng's cell-phone service provider, or by obtaining a warrant under the SCA, 18 U.S.C. § 2703, for the contents of any accounts Feng owns, such as an Internet-based email service or a social-media service, or for text messages sent to and from his phone. Nor did the government seek an SCA order to obtain other potentially useful information from Apple. These records or others may obviate the purported need for Apple's assistance to bypass Feng's passcode.

Finally, as Judge Orenstein noted, the government has failed to make any showing that it has made serious efforts to get the passcode directly from Feng or to have him unlock the phone

[24] The government should not be allowed to supplement the record on necessity in its upcoming reply brief. It is axiomatic that a court need not address arguments or evidence introduced for the first time in a reply brief, *see, e.g., Knipe v. Skinner*, 999 F.2d 708, 710-11 (2d Cir. 1993), particularly where the information "was available to the moving party at the time that it filed its motion and [] is necessary in order for that party to meet its burden," *Revise Clothing, Inc. v. Joe's Jeans Subsidiary, Inc.*, 687 F. Supp. 2d 381, 387 (S.D.N.Y. 2010). Should the government be permitted to introduce new evidence, Apple should be allowed, at the very least, to file a sur-reply addressing those new issues, *see, e.g., Bayway Ref. Co. v. Oxygenated Mktg. & Trading A.G.*, 215 F.3d 219, 227 (2d Cir. 2000) (noting that the district court should permit a nonmoving party to respond to new matters raised in a reply brief before deciding a motion (citation omitted)), and potentially test the veracity of the evidence and information introduced.

for lawful inspection. DE 29 at 35. Likewise, the government has offered no evidence that it has attempted to prompt Feng's memory by showing him a similar phone or having him try to recall the passcode (likely just a 4-digit PIN) by remembering passcodes he commonly uses on other devices.

In conclusion, the government has utterly failed to demonstrate that the requested order is necessary to effectuate the search warrant, including that it exhausted all other avenues for recovering the information it seeks. Before the government demands that Apple do the work of law enforcement, the government must offer evidence that it has performed an "exhaustive search" and that it remains unable to obtain the data it seeks without Apple's assistance. The government has failed to make that showing here and thus its application must be denied.

2. The Remaining Discretionary Factors Under *New York Telephone* Militate Against Compelling Apple's Assistance.

"Closely Related." As Judge Orenstein rightly held, Apple's "assistance "c[an]not be permissibly compelled" because Apple is too "far removed" from the underlying criminal conduct. *N.Y. Tel.*, 434 U.S. at 174. This is because Apple, unlike the public utility in *New York Telephone*, is a private company that does not own or possess the phone at issue, has no connection to the data that may or may not exist on the phone, and is not related to the events giving rise to the investigation. A critical predicate to the application of the All Writs Act in *New York Telephone* and its progeny—but absent here—is the fact that the government was investigating an ongoing crime that was being perpetrated *using the third party's property*.[25] In

[25] The government contends that although Feng has pled guilty, DE 30 at 3, it is still "seeking evidence in an ongoing investigation" of a drug conspiracy, and the contents of the iPhone could be relevant to uncovering the details of this conspiracy, *id.* at 32. But the government's explanation is belied by its actions—waiting more than a year after seizing the iPhone to seek permission to search its contents, and when it finally did so, citing its evidentiary value only in Feng's prosecution. DE 15 at 3; DE 29 at 6. Tellingly, the government did not emphasize the utility of evidence of a conspiracy until after Feng pled guilty, in response to

fact, the government has not cited a single binding case in which the All Writs Act has been invoked to compel a third party to aid in the investigation of a crime to which all defendants have pled and where that third party's property was not being used as an instrumentality in ongoing criminal activity.[26] *See, e.g.*, *id.* at 162 (noting that the subject telephones "had been, were currently being, and would continue to be used in connection" with the suspected offenses); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012) (requiring *defendant* to provide unencrypted copy of hard drive); *United States v. Catoggio*, 698 F.3d 64, 68-69 (2d Cir. 2012) (per curiam) (affirming order restraining *defendant*'s disposition of assets); *Mich. Bell*, 565 F.2d at 386 (authorizing a trap-and-trace of telephones used in ongoing illegal gambling operations in which "gambling operators had established procedures thwarting the effectiveness of . . . wiretaps and pen registers").

The government nevertheless contends that Apple's proximity to the crime—which, again, has already been completed and for which the perpetrator has already pleaded guilty—is established because (1) its facilities were used in the commission of the crime, and (2) its software threatens to obstruct the government's investigation. DE 30 at 32. But this is both incorrect and a distortion of *New York Telephone* and its progeny. To extend that case law to find Apple "closely related" to Feng's criminal conduct in this case would expand the All Writs

---

Judge Orenstein's order that the parties explain why this case was not moot. *See supra* II.D. In addition, all of Feng's co-defendants have already entered guilty pleas. And, in any event, it is wholly speculative that evidence of a conspiracy is only on Feng's iPhone; whatever evidence may have existed when the phone was seized, the likelihood that there is evidence of a present and ongoing conspiracy on a phone that has not been used in nearly two years is vanishingly low.

[26] That is not to say that no order has ever issued compelling third parties to assist the government in such circumstances. But those orders were issued by lower courts in an *ex parte* posture. *See supra* III.B. Lower court orders are, of course, non-binding, and their weight should be further discounted when not the product of adversarial testing. *See District of Columbia v. Heller*, 554 U.S. 570, 623 (2008) ("It is particularly wrongheaded to read [an earlier case] for more than what it said . . . [when] [t]he defendants made no appearance in the case, neither filing a brief or appearing at oral argument . . . .").

Act beyond recognition, to the point at which there would truly be no limit to the government's power to conscript private entities into the service of law enforcement.

The government asserts that Apple's "facilities" were "used" by Feng in committing his crime, yet it fails to explain what facilities it has in mind. Presumably the government is suggesting that because Feng likely used the iPhone *itself*—which "Apple designed, manufactured, and sold," DE 30 at 33—in some manner during the course of his criminal conduct, Apple is closely related to Feng's drug conspiracy. But once the iPhone was sold, Apple never owned or possessed the phone again. And the fact that Apple designed and sold a product that allowed its subsequent owner to communicate about drug transactions hardly renders Apple closely related to that conduct. At bottom, the government's argument that Apple satisfies *New York Telephone*'s proximity requirement is based on Apple's mere insertion of a product into the stream of commerce. *Cf.* DE 29 at 37-38. But as Judge Orenstein rightly observed, interpreting *New York Telephone* to demand nothing more than personal jurisdiction would render the proximity assessment a nullity and violate the oft-expressed admonition that the All Writs Act grants only residual power. *See id.*; *see also supra* III.B.

For this reason, the government relies less on the fact that Feng may have used a device that Apple designed and sold in connection with the commission of his crime than the unsupported contention that Apple is "actively impeding" an investigation by, it would seem, creating software that enables iPhone users to protect their most sensitive personal information and which updates periodically to make devices more secure. DE 30 at 33. Of course, there is nothing active on Apple's part about the security features on the iPhone, as these features require

the owner to activate them. *See id.* at 33.[27] And as for software updates, as with many modern devices, from cars to phones to refrigerators to thermostats, customers buy a combination of hardware and licensed software that updates at regular intervals with the customer's approval. Merely releasing periodic software updates to iPhone users—updates that can be accepted or declined—cannot possibly render Apple on par with telecommunications carriers that have ongoing misconduct occurring on their networks, yet that is precisely what the government seeks to do here. Finally, there is nothing inherently nefarious or obstructionist about building iOS with robust security features. To the contrary, the government has encouraged stronger device encryption in order to protect against the increasing sophistication of cyber criminals, and in the overwhelming majority of cases, such encryption is used for benign purposes. *See* Ex. P [Mike McConnell, Michael Chertoff, & William Lynn, *Why the Fear over Ubiquitous Data Encryption Is Overblown*, Opinion, Wash. Post (July 28, 2015)] ("We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level . . . ."). In none of these respects has Apple "actively imped[ed]" the government's investigation. DE 30 at 33.

Ultimately, it is unnecessary to decipher how exactly the government believes that Apple is closely related to Feng's drug conspiracy because binding case law supports a finding of proximity only where the third party is mediating or hosting the illegal conduct.[28] In *New York Telephone*, for example, a criminal enterprise leveraged the company's telephone network to coordinate and conduct an illegal gambling operation. *See* 434 U.S. at 162. And the Court

[27] In addition, to the extent the government suggests that the existence of a remote wipe feature on Feng's iPhone amounts to Apple actively impeding its investigation, DE 30 at 33, Apple has already informed the government that the remote wipe request will not work on Feng's iPhone, Tr. 32-33.

[28] As noted above, Apple acknowledges the existence of nonbinding *ex parte* orders that have departed from these principles. *See supra* at 20-21.

emphasized that the company was a public utility—not, as the government would have it, to explain the company's duty to assist in law enforcement (which the government contends is shared by private entities)—but because under federal law the company owned and bore a responsibility for maintaining the channels through which the crime was being perpetrated, and did so under the special regulatory oversight applicable to common carriers, 47 U.S.C. § 153. *Id.* at 174; *see also Mountain Bell*, 616 F.2d at 1129; *Mich. Bell*, 565 F.2d at 389.

The same characteristic is present in those rare cases in which an All Writs Act order has issued against a private entity. For instance, in *Hall*, the district court ordered a credit card company to disclose records of transactions that were believed to be used to support a fugitive. 583 F. Supp. at 722. Although the court conceded that the credit card issuer was "not as closely connected with [defendant's] efforts to avoid capture as *New York Telephone* was with the gambling investigation," it nevertheless found the issuer sufficiently close given that it was actively extending credit that was being used to benefit the fugitive. *Id.* at 720; *see also Videotapes*, 2003 WL 22053105, at *3 (ordering apartment complex to provide security videotapes because government had reason to believe fugitive was taking refuge there). Notably, the assistance ordered in these cases was limited to the provision of information already in the third party's possession.

Here, of course, Feng's crime was carried out through the telecommunications networks that connected him to his co-defendants—networks distinct from anything Apple owns or controls. To the extent any incidental use of the iPhone can be deemed relevant, there is no sense in which Apple was hosting or mediating the wrongdoing—indeed, it could not be because, unlike in *New York Telephone*, *Mountain Bell*, *Hall*, or *Videotapes*, Apple does not own

or control the iPhone.[29]

Because Apple is not closely related to the underlying crime, it cannot be compelled to assist in its investigation under the All Writs Act. Indeed, Apple is no more closely related to the underlying crime in this case than it is to music piracy, insurance fraud, or adultery in which an iPhone might play an incidental role; proximity is not established by the happenstance that the offending individual used an Apple device in some way to facilitate his or her conduct—to communicate about drug transactions, to download a song, to send an email to a claims adjustor, or to arrange a rendezvous. At bottom, the government seeks a power that knows no bounds, and that neither the All Writs Act nor *New York Telephone* countenances.

Unreasonable Burden. The Court in *New York Telephone* also made clear that "unreasonable burdens may not be imposed" under the All Writs Act. 434 U.S. at 172. Because the government's request placed no affirmative duty on the telephone company and only required passive assistance—permitting the government to access an unused telephone line to install a pen register—the Court considered it a "meager" burden easily within the ambit of the All Writs Act. *Id.* at 174. Here, however, Apple is being asked to provide affirmative assistance by taking possession of and extracting data from a passcode-protected iPhone. Moreover, unlike the telephone company in *New York Telephone*, Apple has never "offered the government the information needed to bypass an iPhone's passcode security," DE 29 at 40, or performed the type

[29] The government argues that, because Apple "licenses" iOS rather than sells it, the iOS on Feng's iPhone is Apple's property, thus placing this case on all fours with *New York Telephone*. DE 30 at 33 n.7. As Judge Orenstein correctly observed, however, nothing in the record "support[s] an inference that Feng in any way used the licensed software itself—as opposed to the data it allowed Feng to store on the hardware Apple no longer owns—to facilitate his crimes." DE 29 at 32. Moreover, as Judge Orenstein also noted, "[i]n a world in which so many devices, not just smartphones, will be connected to the Internet of Things, the government's theory that a licensing agreement allows it to compel the manufacturers of such products to help it surveil the products' users will result in a virtually limitless expansion of the government's legal authority to surreptitiously intrude on personal privacy." *Id.* at 32 n.26.

of extractions being requested here for its own commercial purposes, *id.* at 39-40 (contrasting this case with *New York Telephone*, in which the company used pen registers for its own business purposes). The few cases that have upheld orders requiring an entity to engage in affirmative conduct involved instances in which the entity already routinely performed the requested task or retained the requested information *outside the context of a court order* (albeit for different purposes). *See, e.g.*, *Mountain Bell*, 616 F.2d at 1126-27 (public utility could be compelled to assist with tracing calls where such traces were "identical to operations routinely undertaken by the company without court order in a variety of circumstances"); *Hall*, 583 F. Supp. at 721 (no undue burden to compel credit card issuer to disclose transaction information that it already maintained); *Videotapes*, 2003 WL 22053105, at *3 (apartment complex had to provide security tapes "already in existence" and in its possession). Here, Apple is being asked to provide affirmative assistance to access data that it does not have in its possession and that is outside the scope of its regular business practices.

In addition, while Apple has said that assisting the government with Feng's iPhone "would not likely place a substantial financial or resource burden on Apple by itself," it has also cautioned that it would "divert[] man hours and hardware and software from Apple's normal business operations," DE 29 at 41; DE 11 at 3, may result in testimonial obligations in order that the evidence obtained from Feng's iPhone may be admissible, DE 11 at 3-4, and will open the floodgates to a deluge of additional requests from the government, *see* DE 29 at 41. Indeed, if this case were only about *a single* iPhone—as the government repeatedly argued in the San Bernardino Matter, but which law enforcement officials have since conceded is not the case—then the burden on Apple would be minor. But law enforcement officials from the Attorney General to the FBI Director and the New York District Attorney have made clear that cases like

the San Bernardino Matter and this case are intended to set a precedent, one that will support an avalanche of similar data access requests from across the country. *See, e.g.*, Ex. Q [Emily Chang, *Interview with Loretta Lynch at RSA Conference* (Mar. 1, 2016) (Lynch explaining that "the fact that there are other phones just shows that in fact this issue is going to grow")]; Ex. E at 15-16 [Comey, *Encryption Hr'g*, Part I (confirming he would "of course" use the All Writs Act to "return to the courts in future cases to demand that Apple and other private companies assist . . . in unlocking secure devices.")]; Ex. R at 10 [New York District Attorney Cyrus Vance, *Encryption Hr'g*, Part II (asserting that there are "thousands of phones" taken as evidence each year and that his office currently has hundreds of devices it cannot access)]. The government's arguments in this case—much like the arguments advanced and then abandoned in the San Bernardino Matter, which involved a different iPhone model and a different operating system—confirm that the burden to Apple must be assessed not through the lens of a single phone or a specific operating system, but in light of the government's unambiguous intent to obtain a precedential ruling that can and will be used to support subsequent orders involving other iPhones running different operating systems and with a variety of security features.

Judge Ornstein rightly recognized that the burden analysis contemplated by *New York Telephone* extends beyond an assessment of the material and labor expenses that would be imposed on Apple if it is ordered to comply with the government's demand. *See* DE 29 at 41 (observing that "the government continues to seek orders compelling Apple's assistance in bypassing the passcode security of more recent models and operating systems, notwithstanding the fact that such requests are more burdensome than the one pending here"). Similarly, here, the Court must consider the practical implications for Apple if the All Writs Act is held to support the boundless power claimed by the government in this case. *See, e.g.*, *Plum Creek*, 608

F.2d at 1289 (considering the cost of future potential injuries). This cumulative burden weighs heavily against granting the government's application.

IV. CONCLUSION

For the foregoing reasons, this Court should affirm Magistrate Judge Orenstein's opinion and deny the government's application for an order compelling Apple's assistance.

Dated: April 15, 2016

Respectfully submitted,

/s/ Theodore J. Boutrous Jr.

Theodore J. Boutrous Jr.*
tboutrous@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

Alexander H. Southwell
asouthwell@gibsondunn.com
Mylan L. Denerstein
mdenerstein@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Marc J. Zwillinger*
marc@zwillgen.com
Jeffrey G. Landis*
jeff@zwillgen.com
ZWILLGEN PLLC
1900 M Street N.W., Suite 250
Washington, D.C. 20036
Telephone: 202.706.5202
Facsimile: 202.706.5298

*Admitted *Pro Hac Vice*

Attorneys for Apple Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of April, 2016, I caused the foregoing document to be filed with the Clerk of the Court for the U.S. District Court for the Eastern District of New York via the Court's CM/ECF system. I further certify that electronic service was accomplished on the following parties:

Robert L. Capers
Saritha Komatireddy
Lauren Howard Elbert
Ameet Kabrawla
U.S. Attorney's Office for the Eastern District of New York
Eastern District of New York
271 Cadman Plaza East
Brooklyn, NY 11201
Telephone: 718.254.7577

/s/ Theodore J. Boutrous Jr.
Theodore J. Boutrous Jr.