

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

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

MEMORANDUM
AND ORDER

15-MC-1902 (JO)

JAMES ORENSTEIN, Magistrate Judge:

The government seeks an order requiring Apple, Inc. ("Apple") to bypass the passcode security on an Apple device. It asserts that such an order will assist in the execution of a search warrant previously issued by this court, and that the All Writs Act, 28 U.S.C. § 1651(a) (the "AWA"), empowers the court to grant such relief. Docket Entry ("DE") 1 (Application). For the reasons set forth below, I conclude that under the circumstances of this case, the government has failed to establish either that the AWA permits the relief it seeks or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion. More specifically, the established rules for interpreting a statute's text constrain me to reject the government's interpretation that the AWA empowers a court to grant any relief not outright prohibited by law. Under a more appropriate understanding of the AWA's function as a source of residual authority to issue orders that are "agreeable to the usages and principles of law," 28 U.S.C. § 1651(a), the relief the government seeks is unavailable because Congress has considered legislation that would achieve the same result but has not adopted it. In addition, applicable case law requires me to consider three factors in deciding whether to issue an order under the AWA: the closeness of Apple's relationship to the underlying criminal conduct and government investigation; the burden the requested order would impose on Apple; and the necessity of imposing such a burden on Apple. As explained below, after reviewing the facts in the record and the parties' arguments, I conclude that none of those factors justifies imposing on Apple the obligation to assist the government's investigation against its will. I therefore deny the motion.

I. Background

On June 6, 2014, a magistrate judge of this court granted the government's applications for a warrant to search the Queens, New York residence of Jun Feng ("Feng"), whom it suspected of involvement in drug trafficking, as well as for warrants to arrest Feng and other suspected coconspirators. *United States v. The premises known and described as 41-21 149th Street, 1st Fl., Queens, NY, 14-MJ-0530* (MDG), DE 2 (search warrant) (sealed); *United States v. Shu Yong Yang, et al.*, 14-CR-0387 (MKB), DE 1 (complaint) & DE 2 (arrest warrants). Feng was arrested on June 11, 2014, and initially ordered detained; he was subsequently released on conditions on July 18, 2014. *Yang*, DE 25 (minute entry); DE 26 (detention order); DE 50 (minute order reflecting release). On July 9, 2014, a grand jury sitting in this district issued an indictment accusing Feng and four other named defendants, together with unnamed others, of conspiracy to traffic in methamphetamine. *See Yang*, DE 47 ¶ 2.

In executing the warrant to search Feng's residence, agents of the United States Drug Enforcement Agency ("DEA") properly seized several mobile devices, including Feng's mobile telephone. *See Govt. II* at 5.¹ As agents later learned, that telephone was an iPhone 5s that used Apple's iOS 7 for its operating system.² *See id.*; *Tr.* at 7.³

¹ To the extent that the Application also constitutes the government's initial memorandum in support of its request for relief, *see id.* at 2, I will alternatively cite it as "Govt. I." I cite other sources of the parties' arguments as follows. *See* DE 11 (Apple's initial memorandum in partial opposition) ("Apple I"); DE 15 (government's reply) ("Govt. II"); DE 16 (Apple's supplemental opposition, addressing additional issues at my request) ("Apple II"); DE 19 (transcript of hearing dated Oct. 26, 2015) ("Tr."); DE 20 (Apple's post-hearing supplemental letter dated Oct. 28, 2015) ("Apple III"); DE 21 (government's post-hearing supplemental memorandum dated Oct. 28, 2015) ("Govt. III").

² The DEA agents never returned the warrant with the inventory of seized items as required. *See* Fed. R. Crim. P. 41(f)(1)(D). I assume that the warrant was executed during the authorized two-week period that expired on June 20, 2014. The date of Feng's arrest – which coincided with the arrests of all of his codefendants – fell within that period, and thus seems likely to have been the date of the search as well.

³ The record does not reveal the precise version of iOS 7 installed on Feng's iPhone, but neither the government nor Apple has suggested that any differences among the several versions of that operating system – as opposed, for instance, to the important differences between iOS 7 on one hand and iOS 8

Over the course of the next year, although the prosecution of Feng and his codefendants moved forward (as did, presumably, the government's investigation of the unknown others mentioned in the indictment), the government apparently did nothing at all to discover what evidence, if any, could be gleaned from Feng's iPhone. Instead, it waited until July 6, 2015, to seek a warrant to search that device and the others seized from Feng's residence. *See United States v. Cellular Telephone Devices Seized On Or About June 11, 2014 From Premises Located At 41-21 149th Street, First Floor, In Queens, NY*, 15-MJ-0610 (VVP), DE 1 (application for warrant to search devices) (the "Device Application"). A magistrate judge of this court granted the latter application and issued a warrant to search the devices that same day. *Id.*, DE 2 (the "Device Warrant"). Like the earlier warrant to search Feng's residence, this warrant set a two-week time limit on its execution. *Id.*

At some point during the following two weeks, the government "initiate[d] the execution of the search warrant [for Feng's iPhone] by attempting to search the device, turning it on and placing it in airplane mode. The [DEA] agents ... began that search but were unable to complete [it] because" the device required a password to allow access to certain information. Tr. at 6. The DEA agents then sought the assistance of the Federal Bureau of Investigation ("FBI"), but remained unable to bypass the iPhone's passcode security. *Id.* at 6-7; *see also* Govt. II at 5.

At that point – after the expiration of the two-week period during which agents were permitted to execute the Device Warrant – the government sought Apple's technical assistance. *See* Govt. II at 6; Tr. at 6. There appears to be no dispute that Apple's response, consistent with its past practice in at least 70 instances, was that it could and would unlock Feng's phone for the agents, but only if a court issued a lawful order requiring it to do so. *See* Govt. II at 6-7; Tr. at 7-8. Also consistent with past

and later versions on the other in terms of the difficulty of bypassing passcode security – has any bearing on the technical issues pertinent to this matter.

practice, Apple provided the agents with the specific technical language it deemed sufficient to make clear its obligation to provide the services that would allow the agents to gain access to the iPhone's passcode-protected data. *See* Govt. II at 6-7; Tr. at 7-8, 56-57.⁴

On October 8, 2015, the government filed the instant Application, together with the proposed order that Apple had helped it draft. Relying exclusively on the AWA (and cases interpreting it) for authority, the government made several pertinent factual assertions beyond those recounted above:

- "Because the iOS device is locked, law enforcement agents are not able to examine the data stored on the iOS device as commanded by the search warrant." Govt. I at 1.
- "[I]n other cases, courts have ordered Apple to assist in effectuating search warrants under the authority of the All Writs Act. Additionally, Apple has complied with such orders." *Id.* at 2.
- "The requested order would enable agents to comply with this Court's warrant commanding that the iOS device be examined for evidence identified by the warrant." *Id.*
- "Examining the iOS device further without Apple's assistance, if it is possible at all, would require significant resources and may harm the iOS device." *Id.* at 2-3.

⁴ The government's assertion that "Apple ... provided the government with specific language to submit to the Court[.]" Govt. II at 2, could be read to suggest that Apple somehow proposed or approved the government's reliance on the AWA as authority for the request. I note, however, that it is only the 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. *See* DE 1-1; Tr. at 57. Also, the reference above to "the iPhone's passcode-protected data" is deliberately circumscribed. It omits information that the agents could, under certain circumstances, access without entering the correct passcode, such as a log of recent telephone calls made or received on the device. *See* DE 15-4 (Govt. II, Ex. D; excerpt from Apple on-line user's manual) ("Allow Access When Locked: Allow access to some features when your device is locked, including Notifications View, Siri, and Control Center."). It also omits other types of data that might be stored on the device (such as information relating to third-party applications that Feng had installed on the device) that could be encrypted or protected by different passcodes and therefore inaccessible to someone using the device's passcode without additional assistance that the government does not seek here. The record does not reveal whether the government's agents, in their attempts to execute the warrant to date, have tried to access information on Feng's device that is not passcode protected and, if so, what they found as a result.

- "[T]he [requested] order is not likely to place any unreasonable burden on Apple." *Id.* at 3.

On October 9, 2015, I issued a Memorandum and Order that declined to rule on the Application *ex parte*, and instead afforded Apple an opportunity to be heard in advance of any decision about the applicability of the AWA in the circumstances of this case. DE 2, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015). I simultaneously directed the Clerk to maintain the Application – but not the Memorandum and Order, which revealed no factual details of the matter – under seal, on the mistaken assumption that its public dissemination could adversely affect an ongoing criminal investigation. DE 3. In its subsequent submission, the government stated that it had never intended to submit under seal either the Application or the proposed order (both of which it attached to its publicly filed legal memorandum), and also noted that the 2015 search warrant authorizing the search of Feng's iPhone was already available on the public docket. *See* Govt. II at 2 n.1 & Ex. A.

Apple submitted its initial opposition to the Application on October 19, 2015; the government replied on October 22, 2015; Apple filed a supplemental response on October 23, 2015;⁵ and I heard oral argument on October 26, 2015. *See* Apple I; Govt. II; Apple II; DE 18 (minute entry). At oral argument, it became apparent that there were a number of factual and legal issues that the government and Apple should have further opportunity to address, and I therefore set a schedule for them to file

⁵ Apple, in its initial submission, took pains to avoid addressing any issue other than the feasibility and burdensomeness of the requested relief – explaining that that was all I had asked it to do. In particular, it did not provide its views on the legal question of whether the AWA empowers the court to grant the Application, and it apparently sought no opportunity to do so later. *See* Apple I at 1 & n.2 ("Apple is not requesting oral argument."). Because I concluded that Apple was in the best position to knowledgeably litigate the legal issue presented here – and in particular, in a better position to do so than the American Civil Liberties Union ("ACLU"), which had offered to submit its own brief on behalf of itself and other *amici curiae*, *see* DE 10 – I asked Apple to file a supplemental response addressing the legal issue and to appear at oral argument, if only to answer my questions; I simultaneously denied the ACLU's motion to file an *amicus* brief. *See* Orders dated Oct. 20, 2015.

post-hearing submissions. DE 18. Apple and the government filed their respective supplemental briefs on October 28, 2015. *See* Govt. III; Apple III.

The accelerated briefing and argument schedule described above was not a reflection of the simplicity of the issues in dispute. Rather, it accommodated the government's interest in resolving the matter (both before me and on review of my decision by a district judge) in sufficient time to use any evidence it might secure with Apple's assistance at Feng's trial, which was then scheduled to begin on November 16, 2015. *See* Govt. II at 4. However, just one day after the oral argument in this case, the court scheduled a proceeding to have Feng enter a new plea; two days later, on October 29, 2015, Feng pleaded guilty pursuant to an agreement with the government. *See Yang*, Scheduling Order dated Oct. 27, 2015; *id.*, DE 119 (transcript of plea allocution dated Oct. 29, 2015) ("Allocution") at 12-13 (confirming Feng's agreement with the government). In notifying me of Feng's plea on the day it was entered, the government wrote that it "persists" in the pending Application, "but in view of the guilty plea, no longer requests expedited treatment." DE 22.

Because the desire to secure potential evidence for Feng's trial was the only basis for seeking Apple's assistance that the government had identified up to that point, *see* Govt. II at 3 ("[t]he government seeks evidence relevant to a defendant's guilt in a federal criminal case"), I promptly directed the government to explain why the Application was not moot. Order dated Oct. 30, 2015. The government responded that same day. It noted that Feng has yet to be sentenced, and that his case therefore remains open – although it did not attempt to explain how any information on the iPhone might alter the advisory sentencing guidelines range that would apply based on factors, including the amount and type of drugs involved in the offense, that the parties agreed the court could take into account. *See* DE 25 at 2; Allocution at 14-16. In addition to relying on the continuing potential need for evidence against Feng, the government also proffered a new theory: it noted that "Feng pleaded guilty

to a narcotics conspiracy, and the government's investigation into that conspiracy is ongoing. The underlying search warrant authorizes the government to seize evidence relating to Feng 'and others,' including 'customers' and 'sources of drugs.'" DE 25 at 1 (quoting Application, Ex. A, Attachment B).⁶

For several months after Feng's plea and the government's letter, this case progressed no further. On February 12, 2016 – apparently unprompted by any development in this case, but just as apparently, in hindsight, reacting to developments elsewhere – Apple filed a letter in response to the government's submission about the procedural viability of the Application in light of Feng's plea. Apple eschewed comment on whether the government's ongoing hunt for unindicted others, or the prospect of Feng's sentencing, sufficed to keep the controversy alive. Instead, Apple alluded to "additional requests similar to the one underlying the case before this Court" and the fact that it has "been advised that the government intends to continue to invoke the All Writs Act in this and other districts in an attempt to require Apple to assist in bypassing the security of other Apple devices in the government's possession." DE 26 (letter dated Feb. 12, 2016) at 1. Based on those similar requests and the anticipation of further motions under the AWA, Apple asserted that this matter "is not moot because it is capable of repetition, yet evading review." *Id.* at 2 (citing *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 190 n.6 (1977)).

I recognized that while Apple's letter identified a sound legal theory, it did not supply a sufficiently particularized factual basis for applying it in this case. Moreover, it was apparent that those

⁶ The pretrial proceedings in Feng's case had lasted for nearly a year after the defendants' arrest when, at a status conference on June 3, 2015, Feng made clear his intention to proceed to trial (notwithstanding the other remaining defendants' announced intentions to enter guilty pleas) and the court indicated a desire to begin the trial in August. *See Yang*, Minute Entry dated June 3, 2015. On July 10, 2015, the court in Feng's case acceded to the parties' need to translate and review extensive recordings in Chinese and set a trial date of November 16, 2015. *See Yang*, Minute Entry dated July 10, 2015. It was only at that point that the government, on July 6, 2015, sought the warrant it seeks to have the court enforce here.

unreported facts might bear on a number of legal issues about which the parties had disagreed at oral argument. I therefore directed Apple to provide, among other things, specific details of the requests it had received from the government during the pendency of this action, the position Apple had taken in response, and the results of those requests. *See* Order dated Feb. 16, 2016. Although I did not require a response until March 1, 2016, Apple supplied the requested information the next day. DE 27 (letter dated Feb. 17, 2016). In that response, Apple identified nine requests filed in federal courts across the country from October 8, 2015 (the date of the instant Application) through February 9, 2016. *Id.* at 2. In each, Apple has been ordered under the authority of the AWA (or has been told that an order has been requested or entered) to help the government bypass the passcode security of a total of twelve devices; in each such case in which Apple has actually received a court order, Apple has objected. *Id.* None of those cases has yet been finally resolved, and Apple reports that it has not to date provided the requested assistance in any of them. *Id.* at 2-3.

In addition to the nine new cases described above, Apple also reported that as recently as February 16, 2016, shortly after my own order of the same date, the United States District Court for the Central District of California had entered an *ex parte* order under the AWA directing Apple

to perform even more burdensome and involved engineering than that sought in the case currently before this Court – *i.e.*, to create and load Apple-signed software onto the subject iPhone device to circumvent the security and anti-tampering features of the device in order to enable the government to hack the passcode to obtain access to the protected data contained therein.

Id. at 1 (citing DE 27-1 (copy of *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M) (the "California" action), Order Compelling Apple, Inc. to Assist Agents in Search (C.D. Cal. Feb. 16, 2016)). On February 22, 2016, the government confirmed that Apple's description of the recent requests could properly be filed on the public docket without jeopardizing any pending criminal

investigation; in doing so, it noted the existence of yet one more case in which a court has ordered Apple to help the government bypass the passcode security of a locked device. DE 28. This matter is therefore one of a dozen pending cases in which the government and Apple disagree as to the court's authority to command Apple to assist the government in defeating the passcode security of devices Apple has manufactured.⁷

II. Discussion

A. Mootness

As a threshold matter, I agree with the government that its Application is not moot as a result of Feng's guilty plea. Whether the government will ever actually use any information it may find on Feng's phone either to litigate the sentencing phase of Feng's prosecution or to identify and prosecute the coconspirators, customers, and suppliers the government is pursuing, is ultimately of no moment. The government enjoys the prerogative to conduct lawful investigations into suspected criminal activity as it sees fit, and in this case it chooses to search for evidence on Feng's iPhone notwithstanding the fact that Feng's guilt has been established. Having made that choice, it is free to take the position it does here, and a ruling on the Application will therefore resolve a live dispute about whether Apple must unwillingly be compelled to provide the assistance the government seeks. The matter is therefore not moot.⁸

⁷ In addition, the government has identified three other closed cases in which a court issued an order under the AWA requiring Apple to extract information from a passcode-protected device, all without objection from Apple. *See* Govt. II at 9-10.

⁸ I do not rely on Apple's assertion that the case is justiciable on the ground that the dispute here is capable of repetition yet evading review. This case would obviously not be moot if Feng had continued to insist on his right to a trial; and there is no reason to suppose that in the dozen pending cases there are none in which Apple's objection to an order under the AWA requiring its assistance can be litigated and resolved before being mooted by a defendant's plea. Indeed, it is entirely possible that some of those cases – such as the *California* action, in which the only known participants in the crime under

B. The All Writs Act

For as long as this nation has had courts established by Congress pursuant to Article III of the Constitution, those courts have been endowed with broad statutory authority to ensure they could effectively carry out the duties of an independent judiciary by issuing the orders necessary to do so – even if Congress had not had the foresight to create all of the procedural mechanisms that might be required. As initially enacted by the First Congress in 1789, the AWA provided:

That all the before-mentioned courts of the United States, shall have power to issue writs of *scire facias*, *habeas corpus*, and all other writs not specially provided for by statute, which may be necessary for the exercise of their respective jurisdictions, and agreeable to the principles and usages of law.

Judiciary Act of 1789, 1 Stat. 73, § 14 (Sept. 24, 1789); *see id.* §§ 1-5 (establishing the courts mentioned in Section 14). That language has been amended only twice in the succeeding centuries, and never in any substantive way. In 1948, when Congress codified federal criminal law in Title 18 of the United States Code, it rendered the statute's text in a more modern style by removing the reference to two specific common law writs, it updated the language to reflect the broader array of federal courts then in existence, it expanded "necessary" to "necessary or appropriate", and it decided (for reasons that I cannot imagine have any impact on this case) to switch the order of words "principles" and "usages":

The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions agreeable to the usages and principles of law.

80 Pub. L. 772, 62 Stat. 683, 944 (June 25, 1948). A year later, Congress merely inserted the word "and" before the word "agreeable". *See* 81 Pub. L. 72, § 90, 63 Stat. 89, 102 (May 24, 1949). Thus, as currently formulated, the AWA provides, in pertinent part:

investigation have died, and where, as a result, there are no defendants with pending charges at all – cannot be concluded without the court first resolving the dispute arising under the AWA.

The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

28 U.S.C. § 1651(a).

The plain text of the statute thus confers on all federal courts the authority to issue orders where three requirements are satisfied:

1. issuance of the writ must be "in aid of" the issuing court's jurisdiction;
2. the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and
3. the issuance of the writ must be "agreeable to the usages and principles of law."

If an application under the AWA meets all three of those requirements, the court "may" issue the requested writ in the exercise of its discretion – but it is never required to do so. *See, e.g., Application of U.S. in Matter of Order Authorizing Use of a Pen Register*, 538 F.2d 956, 961 (2d Cir. 1976), *rev'd on other grounds, United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977); *Morrow v. District of Columbia*, 417 F.2d 728, 736 (D.C. Cir. 1969); *Paramount Film Distributing Corp. v. Civic Center Theatre, Inc.*, 333 F.2d 358, 360 (10th Cir. 1964); *Chemical & Indus. Corp. v. Druffel*, 301 F.2d 126, 129 (6th Cir. 1962). A court deciding whether to take such discretionary action should consider three additional factors:

1. the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction;
2. the reasonableness of the burden to be imposed on the writ's subject; and
3. the necessity of the requested writ to aid the court's jurisdiction (which does replicate the second statutory element, despite the overlapping language).

See N.Y. Tel. Co., 434 U.S. at 174-78.

As set forth below, I conclude that in the circumstances of this case, the government's application does not fully satisfy the statute's threshold requirements: although the government easily

satisfies the statute's first two elements, the extraordinary relief it seeks cannot be considered "agreeable to the usages and principles of law." In arguing to the contrary, the government posits a reading of the latter phrase so expansive – and in particular, in such tension with the doctrine of separation of powers – as to cast doubt on the AWA's constitutionality if adopted. Moreover, I further conclude that even if the statute does apply, all three discretionary factors weigh against issuance of the requested writ, and that the Application should therefore be denied as a matter of discretion even if it is available as a matter of law.

C. Statutory Requirements

1. Aid of Jurisdiction

Controlling case law conclusively demonstrates that the government seeks relief that is in aid of this court's jurisdiction for purposes of the AWA. To be sure, Justice Stevens, in a dissenting opinion in *N.Y. Tel. Co.* (reflecting the views of himself and Justices Brennan, Marshall, and Stewart), persuasively explained the important distinction between the judiciary's interest in authorizing a search and the executive's wholly different agenda in using that authority to gather evidence – and simultaneously demonstrated that the case law interpreting the AWA had consistently reflected that distinction. *See N.Y. Tel. Co.*, 434 U.S. at 186-90 (Stevens, J., dissenting); *id.* at 178 (Stewart, J., concurring in part and dissenting in part) (joining Part II of Justice Stevens' dissent).

The *N.Y. Tel. Co.* majority, however, decisively rejected the dissenters' arguments:

The dissent's attempt to draw a distinction between orders in aid of a court's own duties and jurisdiction and orders designed to better enable a party to effectuate his rights and duties ... is specious. Courts normally exercise their jurisdiction only in order to protect the legal rights of parties. In *Price v. Johnston*, 334 U.S. 266 (1948), for example, the production of the federal prisoner in court was required in order to enable him to effectively present his appeal which the court had jurisdiction to hear. Similarly, in *Harris v. Nelson*, 394 U.S. 286 (1969), discovery was ordered in connection with a habeas corpus proceeding for the purpose of enabling a prisoner adequately to protect his rights. Here, we have held that Fed. Rule Crim. Proc. 41 provided the District Court with power to authorize the FBI to install pen registers. The order

issued by the District Court compelling the Company to provide technical assistance was required to prevent nullification of the court's warrant and the frustration of the Government's right under the warrant to conduct a pen register surveillance, just as the orders issued in *Price* and *Harris* were necessary to protect the rights of prisoners.

Id. at 175 n.23. Thus, regardless of the persuasiveness of any argument to the contrary, I am constrained to conclude that, as a general matter, it would normally be in aid of the court's jurisdiction to order Apple to assist the government in executing a valid warrant to search Feng's device.

Further, the fact that the warrant to be enforced expired long before the government sought to compel Apple's assistance in executing it does nothing to extinguish the court's jurisdiction. Although the general rule is that the government must execute a search warrant no more than fourteen days after its issuance, Fed. R. Crim. P. 41(e)(2)(A)(i), in the context of a warrant to seize electronic storage media such as Feng's device, that time limit "refers to the seizure or on-site copying of the media ... and not to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B). Accordingly, ordering Apple to help the government bypass the passcode security on Feng's device would be in aid of this court's jurisdiction for purposes of the AWA.

2. Necessary or Proper

I likewise readily conclude that the requested order to Apple is "necessary or appropriate" within the meaning of the AWA. "Indeed, '[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it.'" *N.Y. Tel. Co.*, 434 U.S. at 172-73 (quoting *Adams v. United States ex rel. McCann*, 317 U.S. 269, 273 (1942)).⁹

⁹ I explain below, in discussing the statute's "usages and principles" requirement, why I reject the government's assertion that the AWA empowers a court to take any action not prohibited by act of Congress. As the passage from *N.Y. Tel. Co.* quoted above demonstrates, however, the government's position is not wholly divorced from prior judicial interpretation of the Act. I agree that only a Congressional prohibition may place a judicial action beyond the bounds of what would otherwise be "necessary or appropriate in aid of" the court's jurisdiction. But that does not mean that every writ

3. Agreeable to the Usages and Principles of Law

The question whether the AWA permits the relief sought here thus reduces to whether it is "agreeable to the usages and principles of law" to compel Apple – a private party with no alleged involvement in Feng's criminal activity – to perform work for the government against its will. Federal case law offers little if any guidance on how to understand that term in the context of this case.¹⁰ I therefore consider this aspect of the statute in the context of case law that more generally discusses the AWA's overall function as a "gap filler" – that is, a source of interstitial authority that renders it unnecessary for Congress to anticipate every circumstance in which a federal court might properly act to vindicate the rights of parties before it. *See, e.g., Harris*, 394 U.S. at 300 ("the purpose and function of the All Writs Act to supply the courts with the instruments needed to perform their duty") (citations omitted); *Michael v. I.N.S.*, 48 F.3d 657, 669 (2d Cir. 1995) ("[T]he scope of the all writs provision

Congress has not proscribed is necessarily "agreeable to the usages and principle of law." Indeed, ascribing such parallel meaning to the latter clause would strip it of any independent effect, and thereby run afoul of an established rule of statutory construction. *Duncan v. Walker*, 533 U.S. 167, 174 (2001) ("It is our duty 'to give effect, if possible, to every clause and word of a statute.'") (quoting *United States v. Menasche*, 348 U.S. 528, 538-39 (1955)); *cf., Marx v. Gen. Revenue Corp.*, 133 S. Ct. 1166, 1177 (2013) ("The canon against surplusage is not an absolute rule [it] assists only where a competing interpretation gives effect to every clause and word of a statute.") (internal quotations omitted). Thus, the government's attempt to rely on the quoted passage from *N.Y. Tel. Co.* as a basis for satisfying the "usages and principles" prong of the AWA, rather than the "necessary or appropriate" prong to which the Court directly relates it, is entirely misplaced. *See* Govt. III at 7.

¹⁰ The Supreme Court wrote in 1952 that, "[i]n determining what auxiliary writs are 'agreeable to the usages and principles of law,' we look first to the common law." *United States v. Hayman*, 342 U.S. 205, 221 n.35 (1952) (quoting *Price*, 334 U.S. at 281). But that observation – made in the context of determining whether a particular type of writ of habeas corpus was available under common law, and therefore under the AWA – has no bearing on the instant dispute. Similarly, the Tenth Circuit's citation to *Hayman* for the same point in the context of determining the availability of a collateral challenge to a criminal conviction also offers no interpretive assistance here. *See Rawlins v. Kansas*, 714 F.3d 1189, 1196 (10th Cir. 2013) (citing *Hayman*, 342 U.S. at 221 n.35). In both cases, the discussion of the "usages and principles" clause was largely directed to identifying the types of writs that could be so described. Apple does not object that the type of assistance the government seeks here cannot find a close enough antecedent in the common law; the issue here – which *Hayman* and *Rawlins* had no need to address – is whether the issuance of such a writ is an appropriate application of the AWA's gap-filling function.

confine[s] it to filling the interstices of federal judicial power when these gaps threaten[] to thwart the otherwise proper exercise of federal courts' jurisdiction.") (quoting *Pennsylvania Bureau of Correction v. U.S. Marshals Serv.*, 474 U.S. 34, 41 (1985)).

The limits of such gap-filling authority are easily discerned. At one end of the spectrum, the AWA cannot be interpreted to empower courts to do something that another statute already authorizes (but that might have threshold requirements that cannot be satisfied in the circumstances of a particular case). *See Pennsylvania Bureau of Correction*, 474 U.S. at 43. At the other end, the government allows that a court cannot rely on the AWA (or, presumably, anything else) to issue an order that is explicitly or implicitly prohibited under a federal statute. *See Govt. III* at 7.

The gap between those two poles is large indeed, and the crux of Apple's dispute with the government about the meaning of the AWA's requirement that a writ be "agreeable to the usages and principles of law" is whether the statute fills all of that gap, as the government contends, or only some of it. In particular, unlike the government, Apple contends that a court order that accomplishes something Congress has considered but declined to adopt – albeit without explicitly or implicitly prohibiting it – is not agreeable to the usages and principles of law. *See Apple II* at 4; *Apple III* at 4. As explained below, I agree. Before discussing that matter, however, I first briefly consider how this case would come out if, instead of rejecting the government's understanding of the AWA's gap-filling function, I adopted it. Even under that reading of the law, I believe Apple has the better argument – both because it is arguable that CALEA¹¹ explicitly absolves a company like Apple of any responsibility to provide the assistance the government seeks here and also because even if CALEA does not have such an explicit prohibition, it is part of a larger legislative scheme that is so

¹¹ The acronym refers to the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, *codified at* 47 U.S.C. §§ 1001-1010.

comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the statute does not affirmatively prescribe.

a. CALEA

i. The Statute's Purpose and Text

Congress enacted CALEA in 1994 to address its concern that "new and emerging telecommunications technologies pose problems for law enforcement[.]" *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 454 (D.C. Cir. 2000) (quoting H.R. rep. No.103-827 ("CALEA House Report"), pt. 1, at 14 (1994)). It designed the statute "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services[.]" *Id.* (quoting CALEA House Report at 9).¹²

As part of its effort to ensure that the law would not stem technological progress, the legislature included several provisions exempting certain kinds of entities from the more general requirement to assist law enforcement in the execution of court orders authorizing various forms of electronic surveillance. These "Limitations" on CALEA's scope, 47 U.S.C. § 1002(b), fell into three categories. First, Congress limited the ability of law enforcement to prescribe or constrain the services communications companies could offer their customers and the equipment and systems used to market them:

¹² Although designed primarily to preserve the ability of law enforcement agencies to engage in lawful electronic surveillance, the statute was not limited to that topic. For example, it also addressed the responsibilities of private companies to preserve and allow access to records relating to wire and electronic communications. *See, e.g.*, 47 U.S.C. § 1002(a)(2)-(4) (prescribing responsibilities concerning "call-identifying information").

Design of features and systems configurations. This subchapter does not authorize any law enforcement agency or office

(a) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services;

(b) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

47 U.S.C. § 1002(b)(1).

Second, Congress explicitly exempted certain types of businesses from the statute's obligations to assist law enforcement:

Information services; private networks and interconnection services and facilities.

The requirements of subsection (a) of this section do not apply to –

(A) information services; or

(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

Id. § 1002(b)(2).

Finally, Congress largely (but not completely) exempted from CALEA's general requirement of private assistance to law enforcement a requirement that businesses help agents bypass any encryption that might shield communications from surveillance:

Encryption. A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

Id. § 1002(b)(3).¹³

¹³ This provision precludes the government from requiring carriers to build into the encryption measures they make available to their subscribers a "back door" that enables law enforcement access

ii. Application to Construction of the AWA

Both the government and Apple agree that CALEA does not compel a private company such as Apple to provide the kind of assistance the government seeks here. *See* Govt. II at 22; Apple II at 5. They disagree as to why that is so: the government contends that CALEA simply has nothing to say on the matter, while Apple argues that the omission reflects a legislative choice. As explained below, Apple's argument has more merit.

The government suggests that CALEA imposes duties on telecommunications carriers only with respect to what it calls "data 'in motion'" and then adds that "[b]y contrast, this case involves evidence already stored on a cell phone (data 'at rest')." Govt. II at 22; *see also* Govt. III at 9-10.¹⁴ From there, it argues that the statutory language exempting "information services" from comparable duties is irrelevant, regardless of whether Apple qualifies as such a service, because the information it seeks to seize from Feng's iPhone is data "at rest." *See* Govt. II at 22 ("CALEA is entirely inapplicable to the present dispute").

The proposition that CALEA makes a distinction between data "at rest" and "in motion" is largely correct as far as it goes, but ultimately misses the point. Even if Congress did not in any way

to encrypted communications. It does no more than provide that law enforcement is entitled to have carriers assist in securing access to encrypted information where the carrier in making such encryption available, has also retained a decryption key for its own purposes that would allow such access.

¹⁴ In seeking to explain CALEA's purported irrelevance to this case, the government observes that the instant application does not seek "to compel Apple to develop a technical capability that Apple does not already possess." Govt. III at 9. Such more intrusive relief, however, is precisely what the government seeks in the *California* action – relying, as it does here, on the proposition that the requested order is "agreeable to the usages and principles of law." As discussed below, that fact is pertinent to a consideration in this case of the reasonableness of the burden the government seeks to impose on Apple.

regulate data "at rest" in CALEA,¹⁵ it plainly could, and did, enact such legislation elsewhere. *See, e.g.*, 18 U.S.C. § 2703(f)(1) (requiring "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, [to] take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process"). Thus, long before the instant Application was filed, Congress enacted legislation to prescribe the private sector's duties to assist a wide variety of law enforcement investigations – relating to data both "in motion" and "at rest." Those laws defined the extent to which all sorts of service providers had such duties: telecommunications service providers, information service providers, and the providers of wire and electronic communications. None of those laws imposed any obligation on Apple to provide the assistance at issue here, and in particular, CALEA expressly stated that the assistance requirement did not apply to "information services." 47 U.S.C. § 1002(b)(2)(A).¹⁶

The latter point is pertinent because, as Apple persuasively argues, "Apple is substantially engaged in the provision of 'information services' as that term is defined under CALEA, and thus could be considered an information services provider." Apple III at 1 (citing 47 U.S.C. § 1001(6)). As Apple notes:

¹⁵ *But see* 47 U.S.C.A. § 1002(a)(2)(B) (requiring telecommunications service providers to have the ability to provide "call-identifying information" to law enforcement even after a call's conclusion – when, presumably, such information would be "at rest" within the government's meaning).

¹⁶ As a fallback position, the government writes that "even if it were applicable, CALEA addresses a provider's capability to produce information when it receives a court order, not the government's authority to obtain information pursuant to a court order in the first place." Govt. II at 22. Here again, the government fails to take into account the reality that Congress does not always place all related regulations of a given subject into a single section of the United States Code. While it is true enough that a service provider's technical capabilities are prescribed in CALEA, Congress has also elsewhere defined "the government's authority to obtain [the] information [a provider must make accessible] pursuant to a court order in the first place." *See, e.g.*, 18 U.S.C. §§ 2518, 2522 (prescribing requirements for the interception of communications and providing for means to thereupon require the pertinent communications service providers to render the assistance necessary to accomplish such interception).

Under CALEA "information services" means the "offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications," and "includes a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; electronic publishing; and electronic messaging services." [47 U.S.C.] § 1001(6).

Apple is substantially engaged in developing and offering products that provide such capabilities. For example, Apple's iTunes service allows customers to purchase, store, and access music, movies, television shows, games and apps via an Internet-connected Apple device, such as an iPhone[.] iTunes thus constitutes an "information service" under CALEA by providing "a capability for ... acquiring, storing ... [and] retrieving . . . information via telecommunications." *Id.* Similarly, iMessage allows Apple customers (connected over the Internet) to communicate by messages sent and received via their iPhone[.]

Apple III at 1-2.

CALEA thus prescribes for telecommunications carriers certain obligations with respect to law enforcement investigations that it does not impose on a category of other entities – described as "information service providers" – that easily encompasses Apple. Thus, as Apple argues with some justification, "the bounds of mandatory law enforcement assistance were drawn by CALEA, and drawn in such a way to exclude the relief the government seeks." *Id.* at 4.

To be sure, CALEA by itself has limits that render that one statute less than comprehensive. But considered together with other statutes prescribing the extent to which law enforcement may secure access to a wide array of data – both "in motion" and "at rest" – as well as the obligations of some private entities but not others to provide affirmative assistance to such investigations, the statute is easily seen as part of a comprehensive legislative scheme. The absence from that comprehensive scheme of any requirement that Apple provide the assistance sought here implies a legislative decision to prohibit the imposition of such a duty.¹⁷ Thus, even under the government's reading of the AWA,

¹⁷ A similar argument can be made with respect to the various statutes and rules authorizing a court to authorize the seizure of various kinds of evidence. Here again, Congress manifestly knows how to explicitly impose an obligation on private parties to provide assistance to law enforcement in the

I would conclude that while the matter is a close call, the Application seeks an order that is not "agreeable to the usages and principles of law."

b. Statutory Construction

If the best reading of CALEA produces a conclusion that it prohibits the relief the government seeks here, then the Application must be denied even under the government's understanding of what it means for a judicial order to be "agreeable to the usages and principles of law." But if CALEA, considered in the context of a larger statutory scheme, does not erect such a barrier to relief on its own terms, then resolution of the Application turns on whether the gap in laws that the AWA fills is, as the government argues, the entire space between authorizing statutes and legislative prohibitions or if, as Apple would have it, it only reaches to such legislative powers as Congress has not considered and either adopted or rejected. As explained below, I conclude that Apple's position is more consistent than the government's with the rule of statutory construction that requires giving meaning to all statutory words and clauses as well as the rules prohibiting interpretations that produce absurd results or are of suspect constitutionality.

First, as a matter of technical statutory construction, I can find no way to read the statute in a way that gives the required independent meaning to three distinct terms in the AWA – "usages", "principles", and "law" – that conforms to the government's view of the statute. *See, e.g., Duncan*, 533 U.S. at 174 (courts have a "duty to give effect, if possible, to every clause and word of a statute") (quoting *Menasche*, 348 U.S. at 538-539); *United States v. Nordic Vill. Inc.*, 503 U.S. 30, 36 (1992) ("a statute must, if possible, be construed in such fashion that every word has some operative effect"); *Am. Civil*

execution of such court orders. Thus, Congress has explicitly required private parties to assist in the execution of warrants authorizing wiretaps and pen registers, *see* 18 U.S.C. §§ 2518(4), 3123(b)(2), but it has imposed no corresponding obligation on private parties to assist in the execution of search and seizure warrants under Federal Rule of Criminal Procedure 41.

Liberties Union v. Clapper, 804 F.3d 617, 623 (2d Cir. 2015) (courts "must ... strive to avoid interpretations of a statute that would render any phrase or provision superfluous") (citing *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001)).

"[A]greeable to" means, in essence, "consistent with." *See, e.g., Webster's Third New International Dictionary of the English Language Unabridged* at 43 (Merriam-Webster 2002) (defining "agreeable" to mean, among other things, "in harmony or keeping : CONSISTENT, CONSONANT"). Congress could easily have written the AWA to mean what the government says it means simply by requiring that a court's orders under the statute must be "agreeable to the law" – because any action not prohibited by law is, by definition, agreeable to the law.¹⁸ But the AWA requires an order issued under its aegis to be agreeable not merely to some part of the entire body of law, but to the law's "usages" and "principles" – which must mean something else. The most natural reading gives meaning to the whole phrase by limiting the permissible orders to those that not only fail to violate legislative prohibitions, but that also are consonant with both the manner in which the laws were developed (that is, the "principles" that the laws reflect) and the manner in which the laws have been interpreted and implemented (that is, the "usages" of the various laws). Others may propose plausible alternative interpretations of "agreeable to the usages and principles of law."¹⁹ But whatever each of its words may mean in isolation, the rules of

¹⁸ Indeed, later Congresses have endorsed just such simple formulations in approving rules that give the judiciary the flexibility it needs to conduct its business. *See* Fed. R. Crim. P. 57(b) ("A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."); Fed. R. Civ. P. 83(a)(1) (authorizing promulgation of local rules that "must be consistent with – but not duplicate – federal statutes and rules adopted under 28 U.S.C. §§ 2072 and 2075"); Fed. R. Civ. P. 83(b) ("A judge may regulate practice in any manner consistent with federal law, rules adopted under 28 U.S.C. §§ 2072 and 2075, and the district's local rules.").

¹⁹ To date, however, the government has not come up with any such permissible alternative construction, let alone a better one. At oral argument, when I invited the government to reconcile its broad reading of the AWA "with a statute that includes not just agreeable to law but agreeable to principles and usages of law [sic]," Tr. at 38, it acknowledged my concern but then went on to answer a different question by discussing the extent to which a particular statute is sufficiently comprehensive

statutory construction compel me to conclude that their meanings are distinct – and the government's preferred reading of the AWA does not permit that.

Second, the implications of the government's position are so far-reaching – both in terms of what it would allow today and what it implies about Congressional intent in 1789 – as to produce impermissibly absurd results. *See, e.g., United States v. Dauray*, 215 F.3d 257, 264 (2d Cir. 2000) ("A statute should be interpreted in a way that avoids absurd results."); *United States v. Wilson*, 503 U.S. 329, 334 (1992) ("absurd results are to be avoided").

At the heart of the government's reading is the assuredly correct observation that there are any number of ways in which Congress may fairly be said to have considered legislation that does not result in the enactment of legislation, and that as a result the only practical way to discern what is agreeable to the usages and principles of law from what is not is to draw a bright line around what Congress has prohibited – either explicitly or implicitly via the omission of authority from a comprehensive legislative scheme. *See* Govt. II at 24; Tr. at 15, 37. I agree with the government that "[c]ongressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction." *Zino Davidoff v. CVS*, 571 F.3d 238, 243 (2d Cir. 2009) (quoting *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 187 (1994)) (quoted in Govt. II at 24). But the choice is not quite so binary as the government implies: a reliance on outright

as to suggest that its limitations imply a legislative prohibition of other actions. *Id.* at 38-39. The government did not thereafter return to the question of statutory construction, and it similarly deflected the question in its post-hearing submission. *See* Govt. III at 7 (acknowledging the need to interpret the "usages and principles of law" clause as a whole, and citing cases in support of its view on the matter, but offering no argument about how to give independent meaning to both "usages" and "principles" consistent with that view). Moreover, as explained above, *see* n.9, *supra*, the principal authority on which the government relies in that argument – and indeed the source of the sole rationale, namely, that "federal courts may avail themselves of all auxiliary writs 'unless appropriately confined by Congress[']" *id.* (quoting *N.Y. Tel. Co.*, 434 U.S. at 171) – does not actually purport to interpret the AWA's "usages and principles of law" clause, but rather its "necessary or appropriate" clause.

prohibition is not the sole alternative to the chaos of attributing significance to mere legislative inaction. As this case makes clear, the record available to a court considering an application under the AWA will likely have a wealth of information beyond mere congressional inaction – including an array of legislative proposals and hearings that provide a stronger basis for the inferences to be drawn from the ultimate absence of enacted legislation.

As a threshold matter, I respectfully disagree with the government's view of what is and is not practical. The duty of faithful adherence to statutory text does not relieve the courts of the frequent need to make judgments about legislative intent, nor does it restrict them to only such interpretive tools as a dictionary may provide.²⁰ There is no reason that a judge, ably guided by competent counsel for adversarial parties as I am here, cannot compare a proposed order under the AWA with the surrounding body of pertinent laws to determine how consonant the two may be.²¹

²⁰ For example, in the conceptually similar context of preemption analysis, the Second Circuit recently observed that even the absence of a full legislative record, which may impede such analysis, "does not change the fact that a court's primary purpose in statutory interpretation is to discern legislative intent." *Entergy Nuclear Vermont Yankee, LLC v. Shumlin*, 733 F.3d 393, 420 (2d Cir. 2013) (internal quotation marks, citation, and footnote omitted); see also *Loyal Tire & Auto Ctr., Inc. v. Town of Woodbury*, 445 F.3d 136, 145 (2d Cir. 2006) (Sotomayor, J.) (holding, in the context of Interstate Commerce Act preemption, that a court "must consider any specific expressions of legislative intent in the statute itself as well as the legislative history").

²¹ That is precisely what the Supreme Court did in *N.Y. Tel. Co.* Instead of simply observing that no law prohibited the court from ordering the telephone company to make its facilities available to install a pen register – which is all that would have been necessary under the government's reading of the AWA – the Court took pains to explain why such an order was consistent with "more recent congressional actions." 434 U.S. at 176. It discerned what "Congress clearly intended to permit[.]" *id.*, and rested its decision on "the clear indication by Congress that the pen register is a permissible law enforcement tool[.]" *Id.* at 178. The results and opinions in other cases are likewise inherently in tension with the government's understanding of the breadth of the AWA's gap-filling function. See, e.g., *Pennsylvania Bureau of Correction*, 474 U.S. at 39 (denying request for AWA order requiring Marshals Service to transport state prisoners to federal courthouses because the applicable statutory language required such assistance from the custodian "but extends this duty to no other"); *Application of the United States for Relief*, 427 F.2d 639, 644 (9th Cir. 1970) (denying request for AWA order to telephone company to provide needed technical assistance for wiretap because Congress "omitted any reference to judicial power to require" such assistance).

Beyond its unduly pessimistic assumptions about a court's practical ability to properly apply the "usages and principles" clause unless strictly constrained, the government's construction of the AWA produces absurd results in application. If, for example the President sent to Congress a bill explicitly authorizing a court to issue the kind of order the government seeks here, and if every single member of the House and Senate were to vote against the enactment of such a law citing the kinds of data security and personal privacy concerns that Apple now embraces, the government would nevertheless describe the order sought here as permissible because Congress had merely rejected the bill – however emphatically, and however clear its reasons for doing so – rather than affirmatively passing legislation to prohibit the executive branch's proposal. Yet in such circumstances, it would be absurd to posit that the authority the government sought was anything other than obnoxious to the law.²²

An even starker illustration of the absurdity the government's construction produces is that it does not allow a court to deem an action beyond the AWA's reach even if it is an exercise of authority that had formerly been available under a statute that Congress elected to repeal because it was persuaded on policy grounds to retract such authority from the executive. Thus, for example, if communications service providers were to persuade Congress that CALEA had imposed unreasonable burdens on them that threatened their ability to remain in business, Congress could make the choice to repeal that law – thereby removing the statutory obligation to provide certain types of assistance to law enforcement. And yet in the absence of a statute affirmatively prohibiting the

²² A legislature so united in its opposition to a presidential proposal could of course, in an effort to conclusively forestall the possibility that a court might endorse such absurdity, pass a prohibiting statute. But if the President's proposal, while overwhelmingly opposed, nevertheless had the support of the bare minimum number of legislators required to sustain a presidential veto, Congress could defeat the President's proposal but could not enact affirmative legislation prohibiting it. Under such circumstances, however, it would still be easy – and, in my view, correct – for a court to conclude that the proposed order could not fairly be described as agreeable to the usages and principles of law.

government from requiring a company to provide such assistance, the government would read the AWA to nevertheless allow a court to order those same companies to provide precisely the same assistance to law enforcement that Congress had decided no longer to compel.

In short, whatever else the AWA's "usages and principles" clause may be intended to accomplish, it cannot be a means for the executive branch to achieve a legislative goal that Congress has considered and rejected. But because such rejection can take many forms, only one of which (and arguably the least likely in most circumstances) is outright prohibition, the government's argument here is manifestly irreconcilable with the statute.

The government's position also produces a wholly different kind of absurdity: the idea that the First Congress might so thoroughly undermine fundamental principles of the Constitution that many of its members had personally just helped to write or to ratify. Its preferred reading of the law – which allows a court to confer on the executive branch any investigative authority Congress has decided to withhold, so long as it has not affirmatively outlawed it – would transform the AWA from a limited gap-filing statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by Congress's superior ability to prohibit or preempt. I conclude that the constitutionality of such an interpretation is so doubtful as to render it impermissible as a matter of statutory construction.

The AWA was enacted as part of the Judiciary Act of 1789, which Justice O'Connor has described as "the last great event in our Nation's founding" and part of "the triad of founding documents, along with the Declaration of Independence and the Constitution itself[.]" Sandra Day O'Connor, *The Judiciary Act of 1789 and the American Judicial Tradition*, 59 U. Cin. L. Rev. 1, 3 (1990); *see also* Dimitri D. Portnoi, *Resorting to Extraordinary Writs: How the All Writs Act Rises to Fill the Gaps in the Rights of Enemy Combatants*, 83 N.Y.U. L. Rev. 293, 296 (2008) (quoting same and providing further

discussion of the AWA's importance). It is no coincidence that an act of such foundational importance, and so essential to the implementation of the constitutional scheme of a government of limited powers carefully allocated among three separate branches, was enacted during the First Session of the First Congress – because so many of that legislature's members had themselves taken part in creating the Constitution itself. Indeed, more than half of the delegates to the Constitutional Convention who signed the Constitution (as well as several dozen delegates to the various state ratifying conventions) were involved in the enactment of Judiciary Act of 1789.²³

It is wholly implausible to suppose that with so many of the newly-adopted Constitution's drafters and ratifiers in the legislature, the First Congress would so thoroughly trample on that document's very first substantive mandate: "All legislative Powers herein granted shall be vested in a Congress of the United States[.]" U.S. Const. Art. I, § 1. And yet that is precisely the reading the government proposes when it insists that a court may empower the executive to exercise power that the legislature has considered yet declined to allow. It is a reading that thoroughly undermines both the legislature's own prerogative to reject a legislative proposal effectively and efficiently (without the need to affirmatively ban the proposed authority) and the more general protection against tyranny that the Founders believed required the careful separation of governmental powers. *See, e.g., Mistretta v. United States*, 488 U.S. 361, 380 (1989) ("[T]he separation of governmental powers into three coordinate

²³ Seventeen delegates to the Constitutional Convention served as members of the First Congress, including, most tellingly, James Madison – the author of the Federalist papers' explication of the principle of separation of powers. In addition, President Washington, who signed the Judiciary Act into law, had likewise represented Virginia at the Convention. *See* The Federalist Nos. 47, 51 (James Madison); Paul Taylor, *Congress's Power to Regulate the Federal Judiciary: What the First Congress and the First Federal Courts Can Teach Today's Congress and Courts*, 37 Pepp. L. Rev. 847, 868 (2010) (detailing the extensive support for the Judiciary Act of 1789 among member of the First Congress who had been delegates to either the Constitutional Convention or the several state ratification conventions) (citing, *inter alia*, Encyclopedia of American History 145 (Richard B. Morris ed., 6th ed. 1982)); About the Signers, <http://www.constitutionfacts.com/us-constitution-amendments/about-the-signers/> (last visited Feb. 29, 2016).

Branches is essential to the preservation of liberty.... Madison ... said: 'No political truth is certainly of greater intrinsic value or is stamped with the authority of more enlightened patrons of liberty.'") (quoting *The Federalist* No. 47, p. 324 (J. Cooke ed. 1961); case citations omitted).

The proposition that the government's interpretation of the AWA produces such a violation of the separation-of-powers doctrine is not simply a matter of taking an argument to a speculative, albeit logical, conclusion. To the contrary, it reflects what is going on right now, in this case. The Application before this court is by no means singular: the government has to date successfully invoked the AWA to secure Apple's compelled assistance in bypassing the passcode security of Apple devices at least 70 times in the past, *see* Tr. at 8; it has pending litigation in a dozen more cases in which Apple has not yet been forced to provide such assistance; and in its most recent use of the statute it goes so far as to contend that a court – without any legislative authority other than the AWA – can require Apple to create a brand new product that impairs the utility of the products it is in the business of selling. It is thus clear that the government is relying on the AWA as a source of authority that is legislative in every meaningful way: something that can be cited as a basis for getting the relief it seeks in case after case without any need for adjudication of the particular circumstances of an individual case (as the arguments that the government relies on here to justify entering an AWA order against Apple would apply with equal force to any instance in which it cannot bypass the passcode security of an Apple device it has a warrant to search).²⁴

²⁴ Assuming that the power the government believes the AWA to confer on the court can properly be characterized as legislative does not, standing alone, necessarily mean that it runs afoul of the separation of powers doctrine. "Congress may delegate to the Judicial Branch nonadjudicatory functions that do not trench upon the prerogatives of another Branch and that are appropriate to the central mission of the Judiciary." *Mistretta*, 488 U.S. at 388. But as explained above, the government's reading would indeed trench upon the legislature's prerogative, by making it impossible in some circumstances to effectively prohibit the executive from gaining a power it seeks unless it can do so with a veto-proof supermajority.

It is also clear that the government has made the considered decision that it is better off securing such crypto-legislative authority from the courts (in proceedings that had always been, at the time it filed the instant Application, shielded from public scrutiny) rather than taking the chance that open legislative debate might produce a result less to its liking. Indeed, on the very same day that the government filed the *ex parte* Application in this case (as well as a similar application in the Southern District of New York, *see* DE 27 at 2), it made a public announcement that after months of discussion about the need to update CALEA to provide the kind of authority it seeks here, it would *not* seek such legislation. *See* James B. Comey, "Statement Before the Senate Committee on Homeland Security and Governmental Affairs," (Oct. 8, 2015), <https://www.fbi.gov/news/testimony/threats-to-the-homeland> ("The United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time.").

The government's interpretation of the breadth of authority the AWA confers on courts of limited jurisdiction thus raises serious doubts about how such a statute could withstand constitutional scrutiny under the separation-of-powers doctrine. It would attribute to the First Congress an anomalous diminishment of its own authority (to deny a request to increase the executive's investigative powers it deemed inadvisable simply by declining to enact it) as well as an equally implausible intention to confer essentially unlimited legislative powers on the judiciary. Adopting that interpretation

would fly in the face of the doctrine of constitutional avoidance, which "allows courts to *avoid* the decision of constitutional questions" by providing "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts."

Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 808 (2d Cir. 2015) (quoting *Clark v. Martinez*, 543 U.S. 371, 381 (2005)) (emphasis in original); *see also Clark*, 543 U.S. at 380-81 ("If one of [two plausible statutory constructions] would raise a multitude of constitutional problems, the other should prevail – whether or not those constitutional problems pertain to the particular litigant before the Court."). I therefore reject the government's interpretation of the AWA's gap-filling function, and conclude that a judicial order that would confer authority that Congress has considered and decided not to enact is not "agreeable to the usages and principles of law."

Applying that interpretation in this case compels the conclusion that the AWA does not authorize the relief the government seeks. In my initial Memorandum and Order in this case, I discussed at some length the history of Congressional consideration in the decades since CALEA's enactment of updates to the statute that would confer – or withhold – the kind of authority at issue here to compel private actors to assist the government in technologically complex investigations. *See* 2015 WL 5920207, at *1-3.²⁵ After reviewing that history, I concluded that "the absence of any explicit statutory authority for the relief the government seeks cannot be attributed to a failure of legislators to consider such an enactment." *Id.* at *3. Nothing in the subsequent submissions from the government or Apple suggests a basis for abandoning that conclusion. I therefore conclude that what the government seeks here is "to have the court give it authority that Congress chose not to confer." *Id.* at

²⁵ That history includes the FBI's briefing of Congress in 2009 about the so-called "Going Dark" problem and drafting legislation to address it in part by amending CALEA to cover companies such as Apple; then-Senator Biden's 1991 bill requiring companies to ensure law enforcement access to the plain text contents of communications when authorized by law; a legislative hearing before the House Subcommittee on Counterterrorism and Intelligence addressing in part law enforcement agencies' challenges in overcoming technological barriers to accessing data; another hearing before the Senate Judiciary Committee in 2015 entitled "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy" during which the Deputy Attorney General and FBI Director jointly called on Congress to legislate on the matter; and the submission of three separate bills in 2015, each of which would have precluded the government from forcing a private entity such as Apple to provide the kind of assistance at issue here. *See* 2015 WL 5920207, at *1-3.

*1 – and that, for the reasons explained above, granting such a request is not "agreeable to the usages and principles of law."

Accordingly, because the government's Application fails to satisfy the AWA's statutory requirements, I must deny the request for relief regardless of any analysis of the discretionary factors under *N.Y. Tel. Co.* As discussed below, however, consideration of those factors would in any event lead to the same result.

D. Discretionary Factors

1. Closeness

a. Apple's Relationship to Feng's Criminal Activity

In *N.Y. Tel. Co.*, the Supreme Court held that where there was probable cause to believe that a telephone company's own property was "being employed to facilitate a criminal enterprise on a continuing basis[.]" and where the company was "a highly regulated public utility with a duty to serve the public," the company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." 434 U.S. at 174. I explained in the Memorandum and Order why it appeared that the circumstances of this case are materially different. *See* 2015 WL 5920207, at *5. After considering the later-submitted arguments from the government and Apple, I adhere to that view, and conclude that unlike the public utility in *N.Y. Tel. Co.*, Apple is too far removed from Feng's criminal conduct to have any obligation to assist the DEA's investigation.

To the extent that Feng used his iPhone in committing crimes, he used his own property, not Apple's. Unlike the telephone company in *N.Y. Tel. Co.*, which owned the facility used for criminal communications, Apple has no ownership interest in anything that the record reveals Feng used to commit a crime. And unlike the telephone company – "a highly regulated public utility with a duty to

serve the public," 434 U.S. at 174 – Apple is a private entity with no greater duty to serve the public than any other business.

The government argues that Apple's relationship to Feng's criminal activity is sufficiently close, notwithstanding those differences, because, while Feng owned the device itself, he merely licensed from Apple the iOS software on which it runs. *See* Govt. II at 13. But while the government ably demonstrates what the license forbade Feng from doing – he could not lawfully "rent, lease, lend, sell, redistribute or sublicense the iOS Software[,]" *id.* (quoting license agreement ¶ B(3)) – it does not explain the significance of that fact in determining the proximity of Apple's relationship to Feng's conduct. As far as I can discern from the record, Feng did not at any time "rent, lease, lend, sell, redistribute, or sublicense" Apple's software; what he did "sell" or "redistribute" was methamphetamine – a course of conduct in which Apple was not involved. Nor does the record support 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; to the contrary the record contains an explicit description of the ways in which the government believes Feng used his iPhone to commit his crimes as well as the types of evidence the DEA agents expected to find on it. *See* Device Application ¶¶ 7-28 & Attachment B. Nothing in that description even remotely suggests that the licensed software played any meaningful role in Feng's crime comparable to the role the telephone company's property played in the crimes under investigation in *N.Y. Tel. Co.*²⁶

²⁶ If Apple's retention of intellectual property rights in the software deployed in a device sold to the public sufficed to render it sufficiently close, for purposes of the AWA, to any crime committed by any user of such a device, it would eventually render the first discretionary factor under *N.Y. Tel. Co.* a dead letter. As constantly increasing computing power is continually squeezed into ever smaller storage devices, the category of consumer products containing licensed software will continue to grow. In 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.

Ultimately, the government's point is not that Apple in any way facilitated Feng's criminal conduct, but rather that it reaps profits from selling devices (and leasing the software on which those devices run) to a vast group of consumers among whom there are inevitably some criminals. From that premise it draws the following conclusion: "Apple cannot reap the legal benefits of licensing its software in this manner and then later disclaim any ownership or obligation to assist law enforcement when that same software plays a critical role in thwarting execution of a search warrant." Govt. II at 13-14. That opinion may be perfectly defensible as moral precept (however much it may be in tension with the legal system's otherwise broad support for free enterprise), but it has nothing to do with the pertinent legal inquiry.²⁷ Apple had no involvement in Feng's crime, and it has taken no affirmative action to thwart the government's investigation of that crime (a matter discussed in greater detail below). Apple lawfully sold to Feng, as it sells to millions of law-abiding individuals and entities (including the government itself), a product that can effectively secure its stored data for the protection of its owner.²⁸ Feng used that device for criminal purposes and left it locked, and the government says

²⁷ It is no surprise that references to the idea that all citizens have some sort of a duty – moral, if not legal – to assist law enforcement upon demand can occasionally be found in judicial opinions. For example, in an 1895 decision upholding a citizen's right to assist the government in enforcing the law by providing information about suspected criminal activity, the Supreme Court held that "such information given by a private citizen, is a privileged and confidential communication, for which no action of libel or slander will lie[.]" *In re Quarles*, 158 U.S. 532, 535-36 (1895). In introducing the topic, the Court included dicta suggesting – without any citation to authority – that that right is also an obligation. *Id.* at 535 ("It is the duty and the right, not only of every peace officer of the United States, but of every citizen, to assist in prosecuting, and in securing the punishment of, any breach of the peace of the U.S. It is the right, as well as the duty, of every citizen, when called upon by the proper officer, to act as part of the posse comitatus in upholding the laws of his country."). Nothing in *Quarles* suggests that the "duty" to which the Court referred is legal rather than moral.

²⁸ Just as the criminal Feng has done, the United States government has chosen to entrust extremely sensitive communications and secret documents – including those of many of the prosecutors and judges who work in this court – to the passcode protections and other robust data security measures available on a variety of Apple devices. That observation does not mean Apple should have any greater or lesser obligation, as a matter of law or morality, to accede to the demands of law enforcement

it cannot open the lock without Apple's help. Nothing in *N.Y. Tel. Co.* remotely suggests that in such circumstances, Apple is so closely related to the crime under investigation that a court can order its assistance under the AWA.

b. Apple's Relationship to the Government's Investigation

The government alternatively posits that Apple is sufficiently close to the underlying controversy for purposes of the AWA because its "software now thwarts the execution of the search warrant" for Feng's iPhone. Govt. II at 15. That formulation comes after (but subtly reinterprets) an earlier quotation from the opinion in *N.Y. Tel. Co.* As the government notes, in arguing that the court has authority to grant relief under the AWA (as opposed to the distinct question of whether such authority should be exercised as a matter of discretion),

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

Govt. II at 11 (quoting *N.Y. Tel. Co.*, 434 U.S. at 174).

There is no question that the court has the authority under the AWA to compel Apple – or anyone else for that matter – to take action regardless of whether it was involved in the underlying criminal conduct, so long as it does so "under appropriate circumstances." *N.Y. Tel. Co.*, 434 U.S. at 174. But the proposition that Apple's purported ability to "thwart" the government's investigation renders it sufficiently close to the underlying controversy as to make such an order appropriate is ultimately unpersuasive. Apple is not doing anything to keep law enforcement agents from conducting

agencies. But it does highlight the proposition that forcing Apple to compromise the data security measures it offers its customers may adversely affect many who rely on such technology for purposes the government would endorse.

their investigation. Apple has not conspired with Feng to make the data on his device inaccessible.²⁹ More importantly, perhaps, it has not even done what the telephone company did in *N.Y. Tel. Co.* – namely, it has not barred the door to its property to prevent law enforcement agents from entering and performing actions they were otherwise competent to undertake in executing the warrant for themselves.³⁰

Indeed, the government's complaint is precisely that Apple is doing nothing at all. If Feng had not engaged the passcode security on his device, or if the government had been able to secure an order compelling Feng to unlock the phone on pain of contempt sanctions, the government might well be in a position to seize the iPhone's data without Apple's assistance. *See* 2015 WL 5920207, at *5 & n.3.³¹

²⁹ In making this point, I do not simply rest on precise requirements for holding a party liable as a coconspirator. Not only has Apple done nothing wrong in marketing devices with such strong data security features, it has exercised a freedom that Congress explicitly deemed appropriate in balancing the needs of law enforcement against the interests of private industry. Specifically, in writing CALEA, Congress included a provision making clear that the statute "does not authorize any law enforcement agency or office ... to prohibit the adoption of any equipment, facility, service, or feature by ... any manufacturer of telecommunications equipment, or any provider of telecommunications support services." 47 U.S.C. § 1002(b)(1)(B). In other words, CALEA provides that law enforcement agencies cannot do precisely what the government suggests here: dictate to a private company in the business of manufacturing smartphones the extent to which it may install data security features on such devices.

³⁰ In *N.Y. Tel. Co.*, the agents would normally have been able to install the authorized pen register without the company's assistance but for the fact that the subject telephone's wires were so placed as to prevent the agents from gaining surreptitious access. The agents thus needed the telephone company not to provide technical expertise they lacked, but only to step out of the way and let them perform their authorized surveillance on company property. *See* 434 U.S. at 162-63.

³¹ The government argues that a court order compelling Feng to unlock the iPhone would be futile because he claims to have forgotten the passcode. *See* Govt. II at 20. More surprisingly, it takes the position that "[c]ompelled decryption raises significant Fifth Amendment issues and creates risk that the fruit of the compelled decryption could be suppressed." *Id.* at 21. I assume the government is not concerned that such an order of compulsion would violate Feng's Fifth Amendment privilege against self-incrimination. *See* Govt. II at 19 (citing *United States v. Li*, 55 F.3d 325, 329 (7th Cir. 1995) for the proposition that "an [AWA] order may be used to require the production of a handwriting exemplar ... even though the subject may face criminal sanctions as a result of his compliance"); *Com. v. Gelfgatt*, 11 N.E.3d 605, 612 (Mass. 2014) (compelling defendant to enter passcode into encrypted computers did not violate the Fifth Amendment right against self-incrimination); *Schmerber v. California*, 384 U.S. 757, 760-65 (1966) (compelled extraction and analysis of blood sample is not compelled testimony and

Thus, Apple is not "thwarting" anything – it is instead merely declining to offer assistance. There may well be some for whom the distinction between a third-party's active obstruction of law enforcement and its passive refusal to help is meaningless as a matter of policy. But it is hardly meaningless as a matter of legal analysis.³² In any event, the distinction is one that precludes a finding that Apple's relationship either to Feng's crime or to the government's investigation of it is sufficiently similar to the telephone company's corresponding role in *N.Y. Tel. Co.* as to justify an order compelling Apple's assistance.³³

therefore does not violate the Fifth Amendment right against self-incrimination). It may well be, as the government suggests, that "[c]ompelled decryption raises significant Fifth Amendment issues" relating to the due process rights of Feng or anyone else who might be compelled to perform such decryption, but I need not address such concerns to resolve the issue now before the court.

³² The distinction also helps to understand why so many of the cases that the government cites as precedent for using the AWA "in support of warrants in a wide variety of contexts[.]" Govt. II at 11-12, offer little if any useful guidance here. In two of the cases, lower courts simply followed *N.Y. Tel. Co.* to order telephone companies to assist with trap and trace devices – orders wholly comparable in every meaningful respect to the pen register order at issue in *N.Y. Tel. Co.* itself. See *In re Application*, 610 F.2d 1148, 1155 (3d Cir. 1979); *In re Application*, 616 F.2d 1122, 1129 (9th Cir. 1980). In four other cases on the government's list, the subject of the order was in possession of evidence of the crime under investigation and was ordered to produce or allow law enforcement access to that evidence – a circumstance wholly inapposite here, as Apple is not alleged to possess any evidence of Feng's crimes. See *United States v. Doe*, 537 F. Supp. 838, 840 (E.D.N.Y. 1982) (telephone company ordered to produce toll records); *United States v. X.*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (same); *United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (bank ordered to produce credit card records); *In re Application of the United States for an Order Directing X to Provide Access to Videotapes*, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (landlord ordered to provide access to security camera video recordings).

³³ I address below, in the context of analyzing whether the relief sought here is unduly burdensome, the hypothetical example an application under the AWA to compel a drug company that had decided to get out of the business of producing drugs used in executions to supply such drugs to the government if they were otherwise unavailable. At oral argument, the government faulted the hypothetical as "inflammatory," see Tr. at 47, but did not contend that it was unrealistic. Nor could it fairly raise such an objection. Before writing the Court's opinion in opinion in *Glossip v. Gross*, 135 S. Ct. 2726 (2015), Justice Alito posed the following question at oral argument:

JUSTICE ALITO: ... Now, this Court has held that the death penalty is constitutional. It's controversial as a constitutional matter. It certainly is controversial as a policy matter. Those who oppose the death penalty are free to try to persuade legislatures to

c. "Minimum Contacts"

In its post-hearing brief, the government offered no new argument about what Apple has done that renders it close enough to Feng's crime for purposes of *N.Y. Tel. Co.*, but it did posit a new legal standard to apply in considering that discretionary factor. It suggests that all that is required is that Apple have "minimum contacts" – although to what, the government does not say. *See* Govt. III at 6. It wrests that suggestion from the wholly inapposite usage of the phrase in *United States v. Int'l Brotherhood of Teamsters*, 907 F.2d 277, 281 (2d Cir. 1990). As explained below, the argument is unpersuasive.

As another court aptly summarized the nature of the dispute in *Teamsters*:

[T]he All Writs Act was used in *Teamsters* to remove state court litigation so as to aid in the enforcement of a district court's order and to prevent repetitive and burdensome litigation and promote judicial economy, that result was necessary because a consent decree that had been in place for three years was threatened by collateral state lawsuits. The district court determined that an injunction was needed to protect the district court's jurisdiction over the parties to the consent decree, and proceeded under the authority of the All Writs Act.

Nat'l Fuel Gas Supply Corp. v. 138 Acres of Land in Vill. of Springville, Cty. of Erie, State of New York, 186 F. Supp. 2d 339, 345 (W.D.N.Y. 2001).

abolish the death penalty. Some of those efforts have been successful. They're free to ask this Court to overrule the death penalty.

But until that occurs, is it appropriate for the judiciary to countenance what amounts to a guerilla war against the death penalty which consists of efforts to make it impossible for the States to obtain drugs that could be used to carry out capital punishment with little, if any, pain?

Glossip v. Gross, 2015 WL 1929998 (U.S. Apr. 29, 2015) (transcript of oral argument) at *14. If the government can discern in Apple's conduct here a level of obstruction sufficient to allow a court to compel assistance under AWA, Justice Alito's question in *Glossip* would easily provide the basis for a judge to find that a drug company's "guerilla war[fare]" served only to thwart a state's lawful implementation of a constitutionally sound execution, and would therefore make the company eligible for an order of compulsion. The possibility is anything but fanciful.

Thus, in *Teamsters*, there was no question about whether the parties affected by the court's use of an AWA order were too far removed from involvement in the underlying dispute – the question was instead whether the court had personal jurisdiction over those non-parties who were located outside of New York. *See Teamsters*, 907 F.2d at 281. Unsurprisingly, the court answered that question of personal jurisdiction by invoking the applicable constitutional standard for a court's assertion of personal jurisdiction – the "minimum contacts" standard. *See id.* (citing *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)). Here, by contrast, the question is precisely what it was not in *Teamsters*: there is no dispute about the court's personal jurisdiction over Apple, but there is a dispute about whether Apple is too far removed from involvement Feng's conduct to be subject to an order under the AWA.

2. Burdensomeness

The Supreme Court acknowledged in *N.Y. Tel. Co.* that a court exercising its authority under the AWA may not impose "unreasonable burdens" on the subjects of its orders. 434 U.S. at 172. In explaining why compelling the telephone company to help the government install a pen register imposed no such unreasonable burden in that case, the Court wrote the following:

[I]t can hardly be contended that the Company, a highly regulated public utility with a duty to serve the public, had a substantial interest in not providing assistance. Certainly the use of pen registers is by no means offensive to it. The Company concedes that it regularly employs such devices without court order for the purposes of checking billing operations, detecting fraud, and preventing violations of law. It also agreed to supply the FBI with all the information required to install its own pen registers. Nor was the District Court's order in any way burdensome. The order provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the Company and no disruption to its operations.

Id. at 174-75 (citations omitted).

The salient points that the Court highlighted as the basis for finding a lack of unreasonable burdens in *N.Y. Tel. Co.* are virtually all absent here. First, Apple is not a "highly regulated public utility

with a duty to serve the public" – the government does not suggest that it is subject to greater regulation than other businesses, it is not a public utility, and it has a duty is to serve its shareholders rather than the public. Second, Apple has indeed contended that it is in its interest as a private company not to provide the assistance sought here: Apple seeks to succeed in a competitive market by being seen to assume "a leadership role in the protection of its customers' personal data against any form of improper access." Apple I at 4. Further, Apple claims to fear – reasonably or otherwise – that providing the requested assistance in the absence of clear legal authority (as I conclude is lacking) "could threaten the trust between Apple and its customers and substantially tarnish the Apple brand." *Id.*

Third, unlike the pen register at issue in *N.Y. Tel. Co.*, the assistance the government seeks here – bypassing a security measure that Apple affirmatively markets to its customers – is not something that Apple would normally do in the conduct of its own business and is, at least now, plainly "offensive to it." *N.Y. Tel. Co.*, 434 U.S. at 174.³⁴ To be sure, Apple's view of what it finds offensive appears to have changed since the days when it routinely voiced no objection to cooperating with AWA orders, and the government's displeasure with that change is as understandable as it is vehement. But however

³⁴ In considering the burden the requested relief would impose on Apple, it is entirely appropriate to take into account the extent to which the compromise of privacy and data security that Apple promises its customers affects not only its financial bottom line, but also its decisions about the kind of corporation it aspires to be. The fact that the government or a judge might disapprove Apple's preference to safeguard data security and customer privacy over the stated needs of a law enforcement agency is of no moment: in the absence of any other legal constraint, that choice is Apple's to make, and I must take into account the fact that an order compelling Apple to abandon that choice would impose a cognizable burden on the corporation that is wholly distinct from any direct or indirect financial cost of compliance.

late Apple may have come to its current view about the way it wishes to exercise its autonomy, the record offers no reason to question its sincerity.³⁵

Fourth, again unlike the telephone company in *N.Y. Tel. Co.*, which "agreed to supply the FBI with all the information required to install its own pen registers[.]" 434 U.S. at 175, the record suggests that Apple has never offered the government the information needed to bypass an iPhone's passcode security on its own – and would never do so. To the contrary, Apple is clearly staking out the position that as a matter of protecting its customers' privacy and data security (and as a matter of securing the benefits it derives from doing so), it does not want the government or anyone else to have access to the information the government would compel it to use to provide the requested assistance at issue here. Apple has explicitly stated that it will comply with a lawful court order to assist in bypassing the passcode security on Feng's iPhone, *see* Tr. at 10, but it has never hinted that it would prefer to simply let the government have the information necessary to do so.

Fifth, yet again unlike the telephone company in *N.Y. Tel. Co.*, which could install a pen register "with ... minimal effort ... and no disruption to its operations[.]" 434 U.S. at 175, the record

³⁵ I thus respectfully disagree with the government's contention that Apple's objection is not "conscientious" but merely a matter of "its concern with public relations." Govt. III at 5. First, I see no reason why a company that succeeds or fails based largely on its ability to maintain congenial relations with the public – that is, with its potential customers – should not be concerned about public relations. Moreover, for all of the government's manifest outrage, there is simply nothing in the record that leads me to question that Apple's recent stance against being compelled to assist the government in bypassing the security it markets to its customers is anything other than a genuine reflection of both how it perceives its private interest in commercial success and the policy preferences of its leaders. The tension between law enforcement and data security in this case and others like it presents a genuine dilemma for people of good faith – indeed, in congressional testimony on February 25, 2016, the FBI's Director described it as "the hardest question I've seen in government." House of Representatives, Permanent Select Committee on Intelligence, Committee Hearing, 2016 WL 755376 (transcript). The fact that Apple resolves that question in a way not to the government's liking does not mean that it is acting in bad faith, or even that it is necessarily putting selfish interests above the public good. As far as I can discern from the record, it means only that the parties have an honest disagreement about how best to accommodate competing legitimate interests.

demonstrates that bypassing the passcode security of just one iPhone "diverts man hours and hardware and software from Apple's normal business operations." Apple I at 3. And while that burden by itself is not substantial in the case of "a single device in good working order, running an operating system earlier than iOS 8," *id.*, the record of this case makes clear that the burdens the government seeks to impose on Apple under the authority of the AWA are not nearly so limited. The government has already secured such assistance at least 70 times before filing the instant petition, it has a dozen more such applications pending, and it clearly intends to continue seeking assistance that is similarly burdensome – if not far more so – for the foreseeable future. In this context, the government's assurance that "any cumulative burden is minimal and likely to decrease *with regard to the type of relief requested here*[" Govt. II at 16 (emphasis added) is particularly unconvincing: the government predicates its argument on the fact that devices using pre-iOS 8 software are becoming an ever smaller slice of Apple's market. *See id.* But that argument omits the fact that the advent of more recent operating systems has done nothing to slow the government's requests – instead, 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.³⁶

³⁶ Even taking the government's argument at face value, I find it unpersuasive because there are at least two reasons why a court considering the reasonableness of the burdens to be imposed by compelling a private party to assist the government under the AWA should take into account cumulative burdens beyond the financial costs directly associated with carrying out that order in isolation. First, as discussed above, the authority the government asks the court to exercise is essentially legislative in nature – and the record makes clear that the government has chosen to rely on the judiciary to achieve such effectively legislative results. It is therefore all the more important for the court, if it is going to engage in such law-making based on an embrace of the government's understanding of what is "agreeable to the usages and principle of law," to exercise such authority in the same way that a legislature would. Congress typically enacts legislation that imposes ongoing burdens on private parties only after developing a full and transparent record in open hearings about the costs and benefits of the proposed law, based on input from all potential stakeholders. It generally does not (or, at a minimum, should not) impose such burdens based on information received *ex parte*

Thus, the government's argument that the burdens an AWA order here would impose on Apple are as negligible as those imposed on the telephone company in *N.Y. Tel. Co.* cannot withstand scrutiny. The government's remaining arguments against a finding of burden are similarly unpersuasive. The government essentially argues that having reaped the benefits of being an American company, it cannot claim to be burdened by being seen to assist the government. *See* *Govt. II* at 19 (noting the "significant legal, infrastructural, and political benefits" Apple derives from being an American company, as well as its "recourse to the American courts" and to the protection of "American law enforcement ... when it believes that it has been the victim of a crime"); *id.* at 19-20 ("This Court should not entertain an argument that fulfilling basic civic responsibilities of any American citizen or company ... would 'tarnish' that person's or company's reputation.").

Such argument reflects poorly on a government that exists in part to safeguard the freedom of its citizens – acting as individuals or through the organizations they create – to make autonomous choices about how best to balance societal and private interests in going about their lives and their businesses. The same argument could be used to condemn with equal force any citizen's chosen form of dissent. All American citizens and companies "derive significant legal, infrastructural, and political benefits from [their] status [as such,]" *id.* – but that cannot mean that they are not burdened in a legally

and considered in secret proceedings absent some compelling reason not present here. Congress would undoubtedly consider in this context all of the potential harms to Apple, not just the financial ones; a court should do no less. Second, a court's decision in a case such as this, although plainly not controlling in other cases, can nevertheless have some precedential value. It is therefore entirely possible that a decision in this case that did not take into account the cumulative costs Apple faces as the government increases its reliance on the AWA to force it to provide investigative assistance in case after case would effectively limit Apple's ability to have a future court take such rising burdens, no matter how great, into meaningful consideration.

cognizable way when forced unwillingly to comply with what they sincerely believe to be an unlawful government intrusion.³⁷

Similarly, the government's contention that "the burden associated with compliance with legal process is measured on the direct costs of compliance, not on other more general considerations about reputations or the ramifications of compliance[,]" *id.* at 19, is irreconcilable with the opinion in *N.Y. Tel. Co.* itself. The Court in that case did not just cite the lack of financial burden on the telephone company; instead, it took pains to refute the lower appellate court's stated concern about the "severe threat to the autonomy of third parties who for whatever reason prefer not to render such assistance." 434 U.S. at 171. Indeed, part of its showing in that regard was the observation that the company's installation of a pen register would not be "offensive to it" – an observation that would be wholly

³⁷ In its post-hearing submission, the government discusses the significance to this case, and to the Supreme Court's opinion in *N.Y. Tel. Co.*, of Chief Judge Cardozo's observation that "the citizenry may be called upon to enforce the justice of the State, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand." *Babington v. Yellow Taxi Corp.*, 250 N.Y. 14, 17 (1928) (quoted in *N.Y. Tel. Co.*, 434 U.S. at 175). As I pointed out at oral argument, *Babington* involved a state statute that explicitly allowed an officer to conscript private assistance. *Babington*, 250 N.Y. at 16 (quoting N.Y. Penal Law (Consol. Laws, c. 40) § 1848: "A person who after having been lawfully commanded to aid an officer in arresting any person ... willfully neglects or refuses to aid such officer is guilty of a misdemeanor."). In *N.Y. Tel. Co.*, in contrast, no such specific authority justified the government's demand for the telephone company's assistance, and the question was whether the AWA provided such authority. The government assures me that such a distinction "is of no moment." Govt. III at 4. As it explains:

[T]he Supreme Court in *N.Y. Telephone Co.* cited *Babington* to emphasize the more general proposition that it is neither improper nor unusual to expect civilians to assist law enforcement. As the *N.Y. Telephone Co.* opinion confirms, just as there is no impropriety in requiring civilian assistance under a statute, there is likewise no impropriety in requiring civilian assistance under the All Writs Act.

Govt. III at 4.

Such argument misses an important point by conflating substantive policy questions with procedural questions about how policy is set. A legislature is of course free to explicitly authorize law enforcement agents to conscript private assistance under such circumstances as the legislature deems fit. But citizens are under no such obligation in the absence of such legislation, and *Babington* cannot help a court to understand whether the All Writs Act can properly be read to permit a judge, rather than a legislature, to compel such assistance.

irrelevant, if not counter-productive, to a decision intended to establish that the only cognizable burdens under the AWA are financial. Finally, the government makes no effort to explain why cognizable burdens should be so limited: as the Court explained in *N.Y. Tel. Co.*, the AWA does not empower a court to impose any burdens that are "unreasonable" – and it said nothing to suggest that only financial burdens could prove unreasonable.

Finally, I return to the point that the Supreme Court addressed in reversing the Second Circuit's decision in *N.Y. Tel. Co.*: the concern that an AWA order compelling a private party to provide service to the government the non-party finds offensive would "pose a severe threat to [their] autonomy[.]" 434 U.S. at 171. As discussed above, the Court concluded that no such threat was posed in that case by the imposition of an obligation on a public utility to perform for the government a task that it would in any event perform in the pursuit of its own business. But the concern about whether the AWA, as construed by the government, would confer on the judiciary an overbroad authority to override individual autonomy cannot be so easily avoided in this case. Nothing in the government's arguments suggests any principled limit on how far a court may go in requiring a person or company to violate the most deeply-rooted values to provide assistance to the government the court deems necessary.

To try to gauge that limit – and to see if one even exists – I deliberately asked the government at oral argument the provocative question noted above, *see* n.34 *supra*, about whether a court could invoke the AWA to force a drug maker to supply lethal injection drugs notwithstanding the manufacturer's conscientious objection to capital punishment. *See* Tr. at 43-48. That the government had no ready answer at oral argument to a question it deemed so inflammatory was not surprising. But even in its post-hearing submission, the government offers nothing more than deflection: "Resolution of the death penalty hypothetical would depend on the particular law, facts, and circumstances if such

a case were to present itself." Govt. III at 5. That is undoubtedly true, but equally unsatisfactory. If the government cannot explain why the authority it seeks here cannot be used, based on the same arguments before this court, to force private citizens to commit what they believe to be the moral equivalent of murder at the government's behest, that in itself suggests a reason to conclude that the government cannot establish a lack of unreasonable burden.

If, as the government would have it, the only cognizable measure of an unreasonable burden in this case is the extent to which Apple might have unreimbursed financial costs arising directly from the work needed to bypass the passcode security on Feng's iPhone, then granting the requested order would not impose an unreasonable burden. But the category of unreasonable burdens is not nearly so narrow, not even as described in the Supreme Court opinion on which the government primarily relies. Taking into account the several other burdens to which Apple objects – burdens that are no less real or cognizable simply because they are harder to quantify – I conclude that granting the government's Application would impose an unreasonable burden on Apple.

3. Necessity

The government contends that it cannot successfully search Feng's device without Apple's assistance. *See* Govt. I at 1-2; Govt. III at 7 ("The government is unable to perform a safe passcode bypass on its own[.]"). If that assertion is true, the government may be entitled to relief under the AWA if it can satisfy the remaining statutory requirements and discretionary factors. But if it is false – if the government has access to resources that would in fact allow it to vindicate this court's jurisdiction without compelling Apple to take action it finds objectionable – that fact would weigh heavily against granting relief. As the movant, it is the government's burden to establish the factual assertions upon which it claims to be entitled to relief. I conclude that it has failed to do so because of

the conflicting evidence in the record about the availability, from private sources other than Apple, of technology that would allow the government to bypass the passcode security on Feng's device.³⁸

In its Application in this case, the government originally asserted that its agents cannot bypass the passcode security of an Apple iPhone. *See* Govt. I at 1-2. Two months earlier, however, in opposing a suppression motion in an unrelated criminal case in this district, the government said something quite different:

[T]he lack of a passcode is not fatal to the government's ability to obtain the records. That is because [the Department of Homeland Security ("DHS"), 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. In other words, even if HSI agents did not have the defendant's passcode, they would nevertheless have been able to obtain the records stored in the Subject iPhone using specialized software. The software works to bypass the passcode entry requirement and "unlock" the cellular telephone without having to

³⁸ Because I conclude that the government has failed to establish necessity for the reasons set forth below, I need not determine whether its refusal to disclose whether federal intelligence agencies have the ability to unlock Feng's device is an independent basis for finding a lack of necessity. While the government's hesitation to reveal what its intelligence agencies can and cannot do is entirely understandable, and may well be an appropriate exercise of discretion to promote national security, that does not mean that the choice must be cost-free for the government in this litigation. In some contexts, such as where the law imposes an affirmative disclosure obligation on the government, it is reasonable to restrict that obligation to pertinent parts of the executive branch rather than insist that the government is a unitary whole. *See, e.g., United States v. Avellino*, 136 F.3d 249, 255 (2d Cir. 1998) (for purposes of the prohibition against the suppression of materially exculpatory information in a criminal case, imputing to each federal prosecutor constructive knowledge of any information known to any government office "would inappropriately . . . adopt a monolithic view of government that would condemn the prosecution of criminal cases to a state of paralysis") (internal quotation marks and citations omitted). But this case is not a matter of the government, in response to some external obligation, seeking to be excused from an unreasonable burden. It is instead a matter of determining whether the government, in coming forward to seek affirmative relief that requires a factual showing, can be allowed to withhold information that might demonstrate the falsity of its assertion. As a legal matter, a court might determine that an intelligence agency's ability to accomplish the technical task at issue here does not render Apple's assistance unnecessary. But to the extent the government seeks to avoid having a court make that legal decision by offering the unconditional assertion that "[t]he government is *unable* to perform a safe passcode bypass *on its own*[" Govt. III at 7 (emphasis added), it has an obligation to prove that assertion rather than simply tell the court that such inquiry is off limits. *See id.* at 8 ("The government is not required to consult with intelligence agencies[.]").

enter the code. Once the device is "unlocked" all records in it can be accessed and copied.

United States v. Adamou Djibo, 15-CR-0088 (SJ), DE 27 at 5 (government's letter to court dated July 9, 2015). At a hearing on the suppression motion in *Djibo*, the government presented the testimony of a DHS expert who testified that although the "IP-Box" technology on which the government relied was both "fairly new" and "finicky," he and others had succeeded in using that technology to bypass passcode security on some Apple devices, if not the precise kind seized from *Djibo*. See *United States v. Djibo*, --- F. Supp. 3d ----, 2015 WL 9274916, at *6 (E.D.N.Y. Dec. 16, 2015).³⁹

In response to my questions at oral argument about the tension between the factual assertions the government had offered in the two cases, the government proffered yet a third. Specifically, the government wrote:

The government has consulted with the testifying agent in *Djibo*, who noted that the government's ability to bypass the passcode on an iPhone is highly device-specific, and depends in part on the specific hardware and software in place. The investigators in this case have examined the possibility of using various third-party technologies, including the hacking tool referenced in *Djibo*, and determined that, in this case, using such technology on the Target Phone [*i.e.*, Feng's iPhone] presents a non-trivial risk of data destruction. Specifically, the tool, which serially tests various passcodes until detecting the correct one, could activate the "erase data" feature of the iPhone and render the data in the Target Phone permanently inaccessible. By contrast, in this case, Apple has the unique ability to safely perform a passcode bypass on the Target Phone without risking such data destruction.

Govt. III at 8. In short, the government, having previously stated both that it cannot bypass an Apple's passcode security without Apple's help and that it can do so, now says that it depends – and that what

³⁹ The device at issue in *Djibo* was "an iPhone 5 installed with the iOS 8.1.2 operating system." *Id.* The parties appear to agree that the passcode security on that operating system is harder to bypass – even for Apple – than the software (an iteration of iOS 7) installed on Feng's iPhone 5s. Indeed, at the oral argument in this case, Apple stated that while it could indeed bypass the passcode security on Feng's device, it would be impossible to do so on any device running iOS 8 or later versions of the operating system. Tr. at 58. As the public record of the California action reveals, the government now appears to believe otherwise. See DE 27-2 (government's memorandum in the *California* action) at 4-8 (describing proposed method for Apple to use in bypassing passcode security on a device running iOS 9).

it depends on is not just which device and which operating system is in question, but also on which government expert makes the attempt.

In *Djibo*, the result of that morass of conflicting statements was a finding that the government had failed to establish that it would inevitably have succeeded in bypassing the passcode security on Djibo's iPhone. *Djibo*, 2015 WL 9274916, at *11. That result does not remotely establish the proposition the government supports here – namely, that it is impossible for it to bypass the security of an earlier operating system without Apple's help. What it does establish is simply that the government has made so many conflicting statements in the two cases as to render any single one of them unreliable. Because it is the government's burden, as the movant seeking relief, to demonstrate a basis for granting its request, I necessarily conclude that it has failed to establish that the help it seeks from Apple is necessary for purposes of the test under *N.Y. Tel. Co.*⁴⁰

III. Conclusion

In deciding this motion, I offer no opinion as to whether, in the circumstances of this case or others, the government's legitimate interest in ensuring that no door is too strong to resist lawful entry should prevail against the equally legitimate societal interests arrayed against it here. Those competing

⁴⁰ Even accepting at face value the government's most recent statement – that the government has access to third-party technology that might work in this case but that might also risk data destruction – the history recounted above undermines the government's assertion of necessity in a different way. That is, read in the light of its most recent statement, the government's position in *Djibo* was that it would have inevitably discovered the evidence on the defendant's iPhone because it would have used the IP-Box technology to secure it – notwithstanding the risk that doing so might destroy the evidence being sought (the way in which that proposition undermines the government's assertion of inevitable discovery is an issue in *Djibo* but not in this case). If that is so, that means that there are some cases – demonstrably including *Djibo* – in which Apple's help in bypassing an iPhone's passcode security is unnecessary not because the government will inevitably succeed in securing evidence on its own, but rather because the risk of destroying evidence in the attempt to seize it is acceptable. That begs the question, which the government leaves unanswered here, why such a risk was acceptable in prosecuting Djibo but not acceptable in prosecuting Feng. Thus, even taking the government at the most recent of its words, there is no showing that Apple's assistance will accomplish something that the government itself deems to be a necessity.

values extend beyond the individual's interest in vindicating reasonable expectations of privacy – which is not directly implicated where, as here, it must give way to the mandate of a lawful warrant. They include the commercial interest in conducting a lawful business as its owners deem most productive, free of potentially harmful government intrusion; and the far more fundamental and universal interest – important to individuals as a matter of safety, to businesses as a matter of competitive fairness, and to society as a whole as a matter of national security – in shielding sensitive electronically stored data from the myriad harms, great and small, that unauthorized access and misuse can cause.

How best to balance those interests is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago. But that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive. It would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate, and ended it, in 1789.⁴¹

⁴¹ Indeed, as FBI Director Comey observed in the context of the *California* action:

[W]e have awesome new technology that creates a serious tension between two values we all treasure: privacy and safety. That tension should not be resolved by corporations It also should not be resolved by the FBI It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before.... I also hope all Americans will participate in the long conversation we must have about how to both embrace the technology we love and get the safety we need.

James Comey, We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead, Lawfare (Feb. 21, 2016, 9:03 p.m.) <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>. That "long conversation" among "people deciding how we want to govern ourselves in a world we have never seen before" will of course be moot if courts presume to make that decision for the American people based on a perceived assignment of extraordinary authority by 18th Century legislators. Director Comey's salutary call for meaningful public debate can therefore be

Ultimately, the question to be answered in this matter, and in others like it across the country, is not whether the government should be able to force Apple to help it unlock a specific device; it is instead whether the All Writs Act resolves that issue and many others like it yet to come. For the reasons set forth above, I conclude that it does not. The government's motion is denied.

SO ORDERED.

Dated: Brooklyn, New York
February 29, 2016

 /s/
JAMES ORENSTEIN
U.S. Magistrate Judge

achieved only by recognizing that the All Writs Act does not serve as a mechanism for courts to give the executive branch authority it fails to secure from the legislature.