

EMN:LHE/SK
F.#2014R00236

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

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

No. 15-MC-1902 (JO)

----- X

THE GOVERNMENT’S POST-HEARING BRIEF

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

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

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

PRELIMINARY STATEMENT

On October 26, 2015, the Court held a hearing in this matter and heard argument from the parties. The government respectfully submits this post-hearing memorandum to supplement its responses on several of the issues raised at the hearing. For the reasons set forth in its previous reply, see ECF No. 15, at the hearing, and below, the government respectfully requests that the Court grant the government's application and issue the proposed order.

ARGUMENT

A. The All Writs Act may be used to compel third party technical assistance

This Court raised the question whether the All Writs Act may be used to compel a third party to provide a service, not merely to provide information or facilities within its possession. It may.

The All Writs Act confers an auxiliary power upon the courts to effectuate their orders. Courts have “broad power” and “significant flexibility in exercising their authority under the Act.” United States v. Catoggio, 698 F.3d 64, 67 (2d Cir. 2012). Services are not categorically excluded from this power, nor would such an exclusion be consistent with the Act’s breadth and flexibility. Indeed, courts have repeatedly upheld the use of the All Writs Act to require third parties to provide services, such as technical assistance, and perform actions to assist the government. See United States v. New York Telephone Co., 434 U.S. 159, 161 (1977) (requiring phone company to provide facilities and technical assistance with pen register); United States v. Li, 55 F.3d 325, 328 (7th Cir. 1995) (requiring defendant to produce handwriting exemplars); In re Application, 616 F.2d 1122, 1129 (9th Cir. 1980) (requiring phone company to provide information, facilities, and technical assistance to facilitate tracing order); In re Application, 610 F.2d 1148, 1155 (3d Cir. 1979) (requiring phone company to provide information, facilities, and technical assistance to facilitate tracing order, including the installation and continual operation of “card drops and other mechanical or electrical devices” and performance of “manual tracing operations” even though “the execution of a trace may require a more extensive and more

burdensome involvement on the part of the phone company” than the execution of a pen register).

In addition, the Supreme Court in New York Telephone Co. explicitly rejected the phone company’s assertion that “it is extraordinary to expect citizens to directly involve themselves in the law enforcement process.” New York Telephone Co., 434 U.S. at 175 n.24. The Court confirmed that citizens’ “duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions.” Id. In support of this proposition, the Court cited Babington v. Yellow Taxi Corp., 250 N.Y. 14, 17 (1928), in which a police officer had ordered a taxi driver “to chase another car.” It is of no moment that Babington relied on an express statutory provision, and not the All Writs Act, as the basis for requiring a third party’s assistance: the Supreme Court in New York 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 New York 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.

In this case, bypassing the passcode to access the data covered by the Court’s search warrant without risking the permanent loss of that data requires a combination of information in the company’s possession, equipment and facilities at its headquarters, and technical assistance — all of which are within the purview of the All Writs Act.

B. Apple is not raising a conscientious objection

This Court raised the question whether the All Writs Act could be used to compel a third party to provide assistance over a conscientious objection, such as in the case of the death penalty. This Court's concern is reminiscent of the one raised by the intermediate court in New York Telephone Co., which "was apparently concerned that sustaining [the proposed All Writs Act order] would authorize courts to compel third parties to render assistance without limitation regardless of the burden involved and pose a severe threat to the autonomy of third parties who for whatever reason prefer not to render such assistance." 434 U.S. at 171. However, the Supreme Court, in overruling the intermediate court, made clear that the All Writs Act analysis is a highly fact-specific, case-by-case analysis, and fear of potential misuse in another scenario is not a basis for failing to use the powers of the Act in the instant case. Resolution of the death penalty hypothetical would depend upon the particular law, facts, and circumstances if such a case were to present itself. Apple has not raised any objection, in this case or any of the dozens of prior cases like it, based on conscience or principle. Here, the only proffered reason for Apple's objection was its concern with public relations. Even that concern is baseless, however — as Apple's counsel acknowledged at the hearing, if there is "sufficient basis in law" to require Apple's assistance, "then [such assistance] wouldn't undermine customer trust." Hr'g Tr. 60. Therefore, compliance with an All Writs Act order issued by this Court will not unduly burden Apple.

C. Apple has a sufficiently close connection to be subject to the proposed order

This Court raised the question of what it means for a third party to be not “so far removed” from the case. The Supreme Court in New York Telephone Co. did not provide a lengthy explanation of what it means to be not “so far removed from the underlying controversy that its assistance could not be permissibly compelled.” However, the Second Circuit has set forth a standard that is easily met in this matter. In United States v. Int’l Brotherhood of Teamsters, 907 F.2d 277 (2d Cir. 1990), the Second Circuit upheld the use of the All Writs Act to enjoin third parties from initiating collateral litigation that would undermine a federal court’s consent decree. In doing so, the Second Circuit stated that “the All Writs Act requires no more than that the persons enjoined [— the third parties subjected to the All Writs Act order —] have the ‘minimum contacts’ that are constitutionally required under due process.” In this case, Apple’s role in the manufacture and sale of the phone (putting it in “the stream of commerce,” Hr’g Tr. 51), its creation and leasing of the phone’s software thwarting execution of the warrant, and its provision of services to the phone’s owner easily satisfies that “minimum contacts” standard.¹

¹ Apple’s remote wipe feature is one aspect of Apple’s ongoing provision of service to iPhone owners, even when the service can interfere with execution of a warrant. Apple has confirmed that someone activated the remote wipe feature on the Target Phone. Apple subsequently stated in its brief and at the hearing that the remote wipe feature will no longer function at this time. However, Apple also stated that it has not taken any affirmative actions to disable the feature. Hr’g Tr. 32. These representations appear to conflict, and Apple has not further explained why the requested remote wipe cannot take effect.

D. Courts retain All Writs Act authority unless it is confined by Congress

This Court raised the question of what sort of Congressional action precludes All Writs Act authority such that courts are employing that authority consistent with the “usages and principles of law.” 28 U.S.C. § 1651. In New York Telephone Co., the Supreme Court stated that federal courts may avail themselves of all auxiliary writs “unless appropriately confined by Congress.” 434 U.S. at 171 (internal marks omitted). As the case law reflects, courts are confined when Congress has passed an express prohibition of the requested authority or one can be reasonably inferred from a comprehensive statutory scheme. See Pennsylvania Bureau of Corr. v. U.S. Marshals Service, 474 U.S. 34 (1985) (precluding All Writs Act authority to order non-custodian to provide service where statute specifically directed custodian to provide that service); Application of the United States, 427 F.2d 639 (9th Cir. 1970) (precluding All Writs Act authority where there was a comprehensive statutory scheme covering wire interceptions); In re Application of the United States for an Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 294, 326 (E.D.N.Y. 2005) (precluding All Writs Act authority to order an action that was “omitted from a far-reaching and detailed statutory scheme that has received the legislature’s intensive and repeated consideration”). Here, there is no such express or implied prohibition in law.

E. The government is unable to perform a safe passcode bypass on its own

This Court referred the government to briefing and testimony in United States v. Adamou Djibo, No. 15-CR-88 (E.D.N.Y. 2015), suggesting that the government may be able to use third-party services or software to access the data on the Target Phone. The testifying agent in Djibo noted that he had previously used a device that is “not a forensic

tool” but rather a “hacking tool” that is “very finicky” and has “varied success” to access the data on an iPhone 4s running a version of iOS 7. Djibo Tr. at 17-18, 29.

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 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.

F. The government is not required to consult with intelligence agencies

This Court raised the question whether the prosecution team in this case has consulted with every component of the U.S. government, including intelligence agencies, in determining its ability to bypass the passcode on the Target Phone. The All Writs Act does not require such an exercise. Notably, New York Telephone Co. and its progeny do not suggest that criminal prosecutors are required to consult with intelligence agencies or with other components that are not part of the prosecution team before applying for relief under the All Writs Act. This is for good reason — doing so presents practical and legal difficulties attendant to the sensitivity surrounding intelligence capabilities and the legal authority of intelligence agencies. Cf. Kyles v. Whitley, 514 U.S. 419, 437 (1995)

(discovery obligations extend only to those agencies or individuals “acting on the government’s behalf in the case” (emphasis added)); United States v. Stewart, 433 F.3d 273, 275 (2d Cir. 2006) (“[T]he propriety of imputing knowledge to the prosecution is determined by examining the specific circumstances of the person alleged to be an ‘arm of the prosecutor,’ which includes such factors as whether the person was involved with the investigation”).

G. CALEA’s definition of “information service” has no bearing on this case

This Court raised the question whether Apple is an “information service” under CALEA. This issue is purely academic here because the classification of a service as a telecommunications or information service is relevant only for determining whether a provider must possess the technical capability to deliver real-time interceptions or call-identifying information to the government pursuant to a court order. The government is not seeking real-time interceptions or call-identifying information, and it is not seeking to compel Apple to develop a technical capability that Apple does not already possess. CALEA’s distinction between a telecommunications and information service — like CALEA itself — is therefore irrelevant.

CALEA applies only to “telecommunications carriers,” 47 U.S.C. § 1002(a), and it defines a “telecommunications carrier” as an “entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire.” Id. § 1001(8)(A).

CALEA does not apply to “persons or entities insofar as they are engaged in providing information services.” 47 U.S.C. § 1001(8)(C)(i). An “information service” is

defined as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications.” Id. § 1001(6)(A). Included within this definition are services “that permit[] a customer to retrieve stored information from, or file information for storage in, information storage facilities,” and “electronic messaging services.” Id. § 1001(6)(B). A single provider can provide services that are covered by CALEA and other services that are not. See Am. Council on Educ. v. F.C.C., 451 F.3d 226, 233 (D.C. Cir. 2006).

Notably, the exclusion of information services from CALEA was not intended to diminish existing legal authorities applicable to those providers. See H.R. Rep. 103-827 (“House Rep.”) at 18 (“[I]nformation services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order.”) (emphasis added). Instead, the exclusion meant only that the capability requirements imposed by CALEA would apply only to telecommunications carriers. Id. (“Only telecommunications carriers, as defined in the bill, are required to design and build their switching and transmission systems to comply with the legislated requirements.”); see also Am. Council, 451 F.3d at 228 (“Because information-service providers are not subject to CALEA, they need not make their networks accessible to law-enforcement agencies.”).

There is nothing within the language or purpose of CALEA that applies to the facts of this case, and that remains true no matter how Apple, the iPhone, and iOS 7 are classified in terms of telecommunications and information services. It is indisputable, for example, that CALEA has no application or relevance to the government’s ability to access stored data. Instead, CALEA governs the ability of telecommunications providers to

“deliver[] intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization.” 47 U.S.C. § 1002(a). See also House Rep. at 9 (describing the purpose of CALEA as aiming “to preserve the government’s ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies.”).

Nor was CALEA aimed at providers — like Apple, here — with pre-existing capabilities to execute court orders; to the contrary, the aim of the statute was to address the challenges posed by the many telecommunications providers that lacked those capabilities. See House Rep. at 15 (stating that a “company-by-company” approach to compliance issues was “becoming increasingly untenable”).

Simply put, CALEA has no place in this dispute.

