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

15 MISC 1902

MEMORANDUM AND ORDER

15-MC-____ (JO)

JAMES ORENSTEIN, Magistrate Judge:

In a sealed application filed on October 8, 2015, the government asks the court to issue an order pursuant to the All Writs Act, 28 U.S.C. § 1651, directing Apple, Inc. ("Apple") to assist in the execution of a federal search warrant by disabling the security of an Apple device that the government has lawfully seized pursuant to a warrant issued by this court. Law enforcement agents have discovered the device to be locked, and have tried and failed to bypass that lock. As a result, they cannot gain access to any data stored on the device notwithstanding the authority to do so conferred by this court's warrant. Application at 1. For the reasons that follow, I defer ruling on the application and respectfully direct Apple to submit its views in writing, no later than October 15, 2015, as to whether the assistance the government seeks is technically feasible and, if so, whether compliance with the proposed order would be unduly burdensome. If either the government or Apple wishes to present oral argument on the matter, I will hear such argument on October 22, 2015, at 12:00 noon.

The first step in analyzing the application is to determine whether the All Writs Act empowers a court to provide the relief the government seeks. In partial support of its application, the government offers the following quotation: "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Serv.*, 474 U.S. 34, 43 (1985) (quoted in Application at 2). That quotation omits, however, the important qualification that immediately follows it in the same opinion:

> Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling. Although that Act empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize

> them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate.

Id.

Thus, the question becomes whether the government seeks to fill in a statutory gap that Congress has failed to consider, or instead seeks to have the court give it authority that Congress chose not to confer. In a recent article, United States Representative Peter T. King has aptly summarized the pertinent legislative history in this regard:

> Since the 1990s law enforcement has raised concerns that emerging technologies such as digital and wireless communications made it increasingly difficult to conduct court authorized surveillance. At the request of Congress, the Government Accountability Office examined the increasing use of digital technologies in public telephone systems, and found it to be a factor that could potentially inhibit the FBI's wiretap capabilities. To help law enforcement maintain the ability to execute authorized electronic surveillance, Congress enacted the Communications Assistance for Law Enforcement Act [Pub. L. No. 103-414, 108 Stat. 4279, *codified at* 47 U.S.C. §§ 1001-1010 ("CALEA")].
>
> CALEA requires telecom carriers to ensure that if they enable customers to communicate, they will enable law enforcement to conduct court-ordered surveillance. CALEA's requirements were administratively expanded by the FCC in 2006 to apply to broadband Internet access and Voice-Over-Internet-Protocol providers. This rule was subsequently upheld as reasonable by a U.S. Court of Appeals in 2006. However, CALEA's requirements did not cover electronic mail, instant messaging, peer-to-peer communications, or social media.
>
> In 2007 Apple introduced the iPhone, the first widely adopted smart phone, capable of communicating across a number of different platforms, and storing large pieces of data including photographs and video. *CALEA is not viewed as applying to data contained on smart phones, and there has been a great deal of debate about whether it should be expanded to cover this content.*
>
> In 2009, the FBI briefed Congress about the "Going Dark" problem, and drafted legislation to amend CALEA to cover internet companies such as Apple, Facebook, Google, and Twitter that developed communications technologies not covered under the current act.
>
> ...
>
> Draft legislation sought by the FBI was approved by the Justice Department, but ... never sent ... to Capitol Hill. A representative for Senator Patrick Leahy, then

chairman of the Senate Judiciary Committee and an original co-sponsor of CALEA, said in 2012 that, "we have not seen any proposals from the Administration." ...

...

As a Senator, Vice-President Biden introduced the Comprehensive Counter-Terrorism Act of 1991, a bill that corresponded to the FBI's current CALEA reform proposals. That bill provided that companies should "ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law." ...

...

Under an amended CALEA regime, if a court order is required today, one will be required tomorrow as well. The substantive Fourth Amendment law and the Federal Rules of Criminal Procedure and Evidence will not change. The point of amending CALEA is only to make sure that if a wiretap is duly authorized by a judge, it can practically be executed. The sub rosa communications of criminals and terrorists must be legally exploitable by the FBI in order to bring them to justice.

Appearing before my Subcommittee on Counterterrorism and Intelligence, International Association of Chiefs of Police (IACP) President Richard Beary testified about the challenges facing police departments across the country: "Unfortunately, those of us who are charged with protecting the public aren't always able to access the evidence we need to prosecute crime and prevent terrorism even though we have the lawful authority to do so. We have the legal authority to intercept and access communications and information pursuant to appropriate legal processes, but we lack the technological ability to do so." He added, "The law hasn't kept pace with technology, and this disconnect has created a significant public safety problem, which is what we mean when we refer to 'Going Dark.'"

Chief Beary noted that, "Law enforcement is not seeking broad new surveillance capabilities above and beyond what is currently authorized by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the digital communications of all citizens. Rather, we are simply seeking the ability to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders – information of potentially significant consequence for investigations of serious crimes and terrorism[.] [CALEA] needs to be changed to incorporate new communications technologies."

"Critical investigations increasingly rely on digital evidence lawfully captured from smart phones, tablets and other communications devices. [Law enforcement's] inability to access this data, either because we cannot break the encryption algorithm resident in the device, or because the device does not fall under CALEA or the developer has not built the access route, means that lives may well be at risk or lost, and the guilty parties remain free."

Peter T. King, "Remembering the Lessons of 9/11: Preserving Tools and Authorities in the Fight Against Terrorism," 41 J. Legis. 173, 178-80 (2014-2015) (emphasis added; citations omitted).

In addition to the history recounted above, I note two further types of legislative developments this year. First, Senator Ron Wyden, Representative Ted Poe, and a bipartisan group of legislators in the House of Representatives have each introduced bills in 2015 that would preclude the government from forcing a private entity such as Apple to compromise the kind of data security at issue here. *See* Secure Data Act of 2015, S. 135, 114th Cong. (2015); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015).

Second, on July 8, 2015, the United States Senate Committee on the Judiciary held a hearing entitled "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy." The Deputy Attorney General and the Director of the FBI submitted testimony at that hearing noting that while the Justice Department still has not proposed specific legislation on the instant issue, there is a need for Congress and others to craft an approach to balancing privacy and law enforcement interests specifically with respect to the encryption of data on smart phones, among other things. *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, before the S. Comm. on the Judiciary, 114th Cong. (Jul. 8, 2015) (statement of Sally Quillian Yates and James B. Comey).[1]

---

[1] In a similarly-titled article published shortly before his Senate testimony, Director Comey discussed the extent to which companies like Apple should be compelled to ensure law enforcement access to the user content stored on its devices. Pertinent to the instant analysis of the All Writs Act, he wrote:

> Democracies resolve such tensions through robust debate.... It may be that, as a people, we decide the benefits here outweigh the costs and that there is no sensible, technically feasible way to optimize privacy and safety in this particular context, or that public safety folks will be able to do their job well enough in a world of universal strong encryption. Those are decisions Americans should make, but I think part of my job is [to] make sure the debate is informed by a reasonable understanding of the costs.

James Comey, "Encryption, Public Safety, and 'Going Dark,'" Lawfare (July 6, 2015, 10:38 AM), https://www.lawfareblog.com/encryption-public-safety-and-going-dark. Director Comey's view about how such policy matters should be resolved is in tension, if not entirely at odds, with the robust application of the All Writs Act the government now advocates. Even if CALEA and the

It thus appears that Congress enacted a statute in 1994 that understandably did not anticipate later technological advancement and therefore omits from its extensive regulation of private actors the authority to compel the exact kind of assistance to law enforcement the government now seeks. But it also appears that members of the executive and legislative branches have considered updating that statute to allow, among other things, the judicial authorization of the precise investigative technique at issue here – and have not reached a consensus that such action is warranted. In such circumstances, there may not be a "statute [that] specifically addresses the particular issue at hand," *Pennsylvania Bureau of Correction*, 474 U.S. at 43, but it is equally true 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. Rather, this case falls in the murkier area in which Congress is plainly aware of the lack of statutory authority and has thus far failed either to create or reject it. Under such circumstances, it is far from obvious that the reasoning in *Pennsylvania Bureau of Correction* supports the proposition that the relief the government seeks is available under the All Writs Act.

The government also cites *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). In that case, the Supreme Court held that the All Writs Act empowered the district court to compel the New York Telephone Company to install a pen register to effectuate a search warrant. But as the court's opinion demonstrates, the circumstances were quite different:

> [The district court] found that there was probable cause to believe that the [Telephone] Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis. For the Company, with this knowledge, to refuse to supply the meager assistance required by the FBI in its efforts to put an end to this venture

---

Congressional determination not to mandate "back door" access for law enforcement to encrypted devices does not foreclose reliance on the All Writs Act to grant the instant motion, using an aggressive interpretation of that statute's scope to short-circuit public debate on this controversy seems fundamentally inconsistent with the proposition that such important policy issues should be determined in the first instance by the legislative branch after public debate – as opposed to having them decided by the judiciary in sealed, *ex parte* proceedings.

threatened obstruction of an investigation which would determine whether the Company's facilities were being lawfully used.

Moreover, it 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.

Finally, we note, as the Court of Appeals recognized, that without the Company's assistance there is no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished. The FBI, after an exhaustive search, was unable to find a location where it could install its own pen registers without tipping off the targets of the investigation. The provision of a leased line by the Company was essential to the fulfillment of the purpose – to learn the identities of those connected with the gambling operation – for which the pen register order had been issued.

The order compelling the Company to provide assistance was not only consistent with the Act but also with more recent congressional actions. As established [above], Congress clearly intended to permit the use of pen registers by federal law enforcement officials. Without the assistance of the Company in circumstances such as those presented here, however, these devices simply cannot be effectively employed. Moreover, Congress provided in a 1970 amendment to Title III that "[a]n order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier ... shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively ...." 18 U.S.C. § 2518(4). In light of this direct command to federal courts to compel, upon request, any assistance necessary to accomplish an electronic interception, it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy. We are convinced that to prohibit the order challenged here would frustrate the clear indication by Congress that the pen register is a permissible law enforcement tool by enabling a public utility to thwart a judicial determination that its use is required to apprehend and prosecute successfully those employing the utility's facilities to conduct a criminal venture.

Id. at 174-78.

There are several ways in which the circumstances of this case differ in material respects from those of *New York Tel. Co.* First, in the latter case, the government needed assistance in effectuating a court order to secure information from the Telephone Company's own facility. Here, by contrast, Apple manufactured the device at issue, but apparently does not own it.[2]

Second, unlike the Telephone Company, Apple is not "a highly regulated public utility with a duty to serve the public[.]" It is a private-sector company that is free to choose to promote its customers' interest in privacy over the competing interest of law enforcement. Indeed, whereas in *New York Tel. Co.* "it [could] hardly be contended that the Company ... had a substantial interest in not providing [the requested] assistance," it is entirely possible, if not likely, that Apple has thus far made a deliberate decision to balance those competing interests in favor of its customers' privacy preferences, as discussed further below. Similarly, unlike the Telephone Company, which as the Supreme Court noted, regularly used pen registers for its own business purposes, there is nothing in the record to suggest that Apple has or wants the ability to defeat customer-installed security codes to access the encrypted data that its customers store on Apple devices after purchasing them.

Third, the Court in *New York Tel. Co.* explained why there was simply no practicable alternative in that case to requiring the Telephone Company to provide a pen register – no other method was available to secure the information that the lower court had already determined should lawfully be made available to the government. That is not the case here: one potential alternative to forcing Apple to try to decrypt the device at issue, and one that may well be more effective, is to compel the device's owner or user to unlock the phone for lawful inspection, on pain of coercive contempt sanctions.[3]

---

[2] Indeed, the record is not even clear that Apple *can* now unlock the device at issue. *See* Application at 1 ("Apple ... *may* be capable of retrieving the data") (emphasis added).

[3] I need not and do not consider the slightly different alternative of an order requiring the owner to reveal the passcode that unlocks the device. The owner may arguably have a Fifth Amendment privilege to refuse to reveal the code, but could not have such a privilege to withhold stored data by

Fourth, the Supreme Court explained at length in *New York Tel. Co.* that requiring the Telephone Company to assist in installing a pen register was manifestly consistent with then-recent Congressional enactments to provide law enforcement with just that investigative tool and to require telephone companies to provide assistance to law enforcement agencies in deploying the surveillance techniques that Congress placed at their disposal. Here, by contrast, Congress has done nothing that would remotely suggest an intent to force Apple, in the circumstances of this case, to provide the assistance the government now requests. To the contrary, Congress has failed to act on concerns expressed by the Justice Department and the FBI about the lack of such legislation, and several of its members have introduced legislation to prohibit exactly what the government now asks to the court to compel. For all these reasons, I conclude that the opinion in *New York Tel. Co.* does not support the government's motion.

In reaching that conclusion, I respectfully disagree with the one other court that I know to have addressed the precise issue presented here. *See In re XXX, Inc.*, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014).[4] In granting the similar application in that case, the court relied on *New York Tel. Co.* and

---

secreting it in such a way that law enforcement could not gain access. Likewise, I do not offer any view on the extent to which, if any, the act-of-production doctrine might require a grant of immunity for any testimonial information that the owner would convey by unlocking the device in the government's possession. *Cf. United States v. Hubbell*, 530 U.S. 27 (2000); *United States v. Doe*, 465 U.S. 605 (1984); *Fisher v. United States*, 425 U.S. 391 (1976); *United States v. Bondo*, 2015 WL 1518987, at *6 (A.F. Ct. Crim. App. Mar 18, 2015) ("We leave as unresolved whether a properly issued warrant may compel a suspect to produce a password."); *United States v. Hatfield*, 2010 WL 1423103 (E.D.N.Y. Apr. 7, 2010); *In re Boucher*, 2009 WL 424718 (D. Vt. 2009); *see also United States v. Furman*, 2015 WL 1061956, at *2 (D. Minn. Mar. 11, 2015) (government obtained password for locked device by asking defendant for it); *United States v. Graham*, 2014 WL 2922388, at *3 (same). The Application does not reveal whether the government knows the identity of the device's owner or user; if it does not, the availability of such compulsion would plainly not be a viable alternative in this case, even if it would be in others.

[4] The government represents, without providing citations, "that in other cases, courts have ordered Apple to assist in effectuating search warrants under the authority of the All Writs Act [and that] Apple has complied with such orders." Application at 2. I have no doubt that the representation is correct, but *In re XXX* is the sole such published decision I have been able to find (although that decision does not reveal whether the private company involved was Apple).

compared the assistance sought there (and here) to the kind of technical assistance deemed to be not unreasonably burdensome in other cases:

> Case law reflects that orders providing technical assistance of the kind sought here are often not deemed to be burdensome. *See, e.g., Application of U.S. for an Order Authorizing an In–Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1132 (9th Cir. 1980) (tracing of a telephone call conducted through an "electronic or mechanical device" rather than manually); *United States v. Hall*, 583 F. Supp. 717, 721 (E.D. Va. 1984) (records that could be generated by "punching a few buttons"); *see also New York Telephone Co.*, 434 U.S. at 177 (assistance "in the installation and operation of" a pen register). Case law also reflects that in some instances parties subject to the writ should be compensated for their expenses. *See, e.g., Application of U.S. for an Order Authorizing an In–Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d at 1133 (court should consider whether third party will be "fully compensated for the services provided"); *Application of U.S. for Order Authorizing Installation of Pen Register or Touch–Tone Decoder & Terminating Trap*, 610 F.2d 1148, 1156 (3d Cir. 1979) (third party would "be compensated 'at the prevailing rates' for its services").

In re XXX, Inc., 2014 WL 5510865, at *2. Based on that analysis, the court granted the government's application, with the proviso that the manufacturer could seek relief from the order within five days if it deemed compliance to be unreasonably burdensome. *Id.* at 3.

The court in *In re XXX, Inc.* implicitly concluded that the burden of compliance for the private actor at issue was limited to the physical demands and immediate monetary costs of compliance. Likewise, in this matter, the government opines that the order it requests "is not likely to place any unreasonable burden on Apple." Application at 3. I am less certain. The decision to allow consumers to encrypt their devices in such a way that would be resistant to ready law enforcement access was likely one that Apple did not make in haste, or without significant consideration of the competing interests of public safety and the personal privacy and data security of its customers. *See, e.g.*, Ellen Nakashima, *Tech Giants Don't Want Obama To Give Police Access To Encrypted Phone Data*, Washington Post, May 19, 2015. It may reflect an analysis of Apple's business prospects that persuaded the company that failing to provide its customers with the kind of privacy protection the government now seeks to overcome would have long-term costs that outweighed the benefits of a technological approach more

to the government's liking. Thus, without hearing from Apple, I cannot assume that forcing it to modify that decision would not impose an unreasonable burden. *Cf. In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1145 (9th Cir. 2003) ("The obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business....") (interpreting CALEA and the All Writs Act in light of the opinion in *New York Tel. Co.*).

In short, I conclude that the authorities on which the government relies do not support the conclusion that the All Writs Act permits the relief that the government seeks. That does not necessarily mean, however, that such relief is unavailable under the statute. While the preceding analysis strongly suggests that granting the instant motion would be inconsistent with the purpose of the All Writs Act as interpreted in the cases discussed above, one important missing piece of the analysis is the extent to which Apple would find the requested order burdensome. Indeed, regardless of whether I were inclined to grant or deny the motion at this point, I would need such information, as "[C]ourts have held that due process requires that a third party subject to an order under the All Writs Act be afforded a hearing on the issue of burdensomeness prior to compelling it to provide assistance to the Government." *In re XXX, Inc.*, 2014 WL 5510865, at *2 (citing *In re Installation of a Pen Register or Touch-Tone Decoder & a Terminating Trap*, 610 F.2d 1148, 1157 (3d Cir. 1979); *United States v. Mountain States Tel. & Tel. Co.*, 616 F.2d 1122, 1132-33 (9th Cir. 1980)).

Accordingly, for the reasons set forth above, I temporarily defer ruling on the instant application and instead respectfully direct the government to serve its application and this Memorandum and Order on Apple forthwith. Apple shall provide a written response no later than October 15, 2015. The government may submit a written reply. If either the government or Apple

wishes to present oral argument on the matter, I will hear such argument on October 22, 2015, at 12:00 noon.

SO ORDERED.

Dated: Brooklyn, New York
October 9, 2015

/s/
JAMES ORENSTEIN
U.S. Magistrate Judge