2018 WL 1964588
United States District Court, N.D. California.

UNITED STATES OF AMERICA, Plaintiff,
v.
RYAN MICHAEL SPENCER, Defendant.

Case No. 17-cr-00259-CRB-1
|
04/26/2018

CHARLES R. BREYER, United States District Judge

ORDER DENYING [DKT. 73] MOTION FOR RELIEF FROM ORDER OF MAGISTRATE JUDGE

***1** Ryan Michael Spencer moves for relief from an order by a magistrate judge compelling him to decrypt several electronic devices. In re Search of a Residence in Aptos, Calif. 95003, No. 17-mj-70656-JSC, 2018 WL 1400401 (N.D. Cal. March 20, 2018). Because the magistrate judge properly applied the foregone conclusion doctrine to the facts of the case, the motion is DENIED.

I. BACKGROUND

On April 26, 2017, a magistrate judge authorized a warrant for the FBI to search a residence believed to be inhabited by Spencer. Specifically, the warrant authorized the search of the premises and any computers, storage media, routers, modems, and network equipment contained within, as well as Spencer himself, for evidence of child pornography.

The FBI searched the residence and seized 12 electronic media items. It determined that some of these contained child pornography. However, several of the devices were encrypted, and their contents were therefore inaccessible. The United States sought an order under the All Writs Act, 28 U.S.C. § 1651, compelling Spencer to decrypt three of these devices: a smartphone, a laptop, and an external hard drive. Spencer admitted ownership of the smartphone and laptop, and provided passwords to bypass the lock screens (though not to decrypt portions of the devices' hard drives).

The external hard drive was seized from the same desk as the laptop. Spencer said he owned a hard drive matching the description of the one seized, and that he had encrypted the hard drive using the same encryption software as that found on the recovered drive.

The magistrate judge granted the government's application on March 20, 2018, ordering Spencer to aid in decrypting the three devices. In re Search of a Residence in Aptos, Calif. 95003, No. 17-mj-70656-JSC, 2018 WL 1400401 (N.D. Cal. March 20, 2018). Spencer filed a motion for relief from the order on April 16. See Mot. for Relief (dkt. 73).

II. LEGAL STANDARD

A party may file a motion for relief with the district court from a dispositive pre-trial ruling by a magistrate judge. Fed. R. Crim. P. 59(b)(2). A district court's review of a dispositive order by a magistrate judge is de novo. Fed. R. Crim. P. 59(b)(3).

The Fifth Amendment to the United States Constitution provides that "No person...shall be Compelled in any criminal case to be a Witness against himself." It applies "only when the accused is compelled to make a Testimonial Communication that is incriminating." Fisher v. United States, 425 U.S. 391, 408 (1976). Accordingly, the Fifth Amendment is not violated whenever the government compels a person to turn over incriminating evidence. Id. at 409. Instead, it is only implicated when the act of production itself is both "testimonial" and "incriminating." Id. at 410.

The act of production is neither testimonial nor incriminating when the concession implied by the act "adds little or nothing to the sum total of the Government's information by conceding that he in fact has the [evidence]"—that is, where the information conveyed by the act of production is a "foregone conclusion." Id. at 411. It is important to stress the limited scope of the "foregone conclusion" rule. It only applies where the testimony at issue is an implied statement inhering in the act of production itself. See United States v. Apple MacPro Computer, 851 F.3d 238, 247 (3d Cir. 2017). Otherwise, the government cannot compel a self-incriminating statement, regardless of whether the contents of the statement are a "foregone conclusion." See Fisher, 425 U.S. at 429 (Brennan, J., concurring) (whether testimony is considered incriminating under the Fifth Amendment does not "turn on the strength of the Government's case").

***2** For instance, the government could not compel Spencer to state the password itself, whether orally or in

writing.[1] But the government is not seeking the actual passcode. Rather, it seeks the decrypted devices. Spencer argues that production of the devices would not fall within the act-of-production doctrine because producing the devices would require him to enter the decryption password. In other words, Spencer argues that because the government cannot compel him to state the passwords to the devices, it cannot compel him to decrypt the devices using the passwords, either. This argument has some superficial appeal, and finds support in a dissent by Justice John Paul Stevens, who once contended that a defendant could "not...be compelled to reveal the combination to his wall safe" either "by word or deed." Doe, 487 U.S. at 219 (Stevens, J., dissenting) (emphasis added). While the analogy is not perfect, we may assume that storing evidence in encrypted devices is equivalent to securing items in a safe protected by a combination, and that Justice Stevens' reasoning applies equally to the situation at hand. See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

But a rule that the government can never compel decryption of a password-protected device would lead to absurd results. Whether a defendant would be required to produce a decrypted drive would hinge on whether he protected that drive using a fingerprint key or a password composed of symbols. See New York v. Quarles, 467 U.S. 649, 671 (1984). Similarly, accepting the analogy to the combination-protected safe, whether a person who receives a subpoena for documents may invoke the Fifth Amendment would hinge on whether he kept the documents at issue in a combination safe or a key safe. See Doe, 487 U.S. at 210 n.9. But this should make no difference, because opening the safe does not require producing the combination to the government. Whether turning over material, either in the form of documents or bits, implicates the Fifth Amendment should not turn on the manner in which the defendant stores the material.

So: the government's request for the decrypted devices requires an act of production. Nevertheless, this act may represent incriminating testimony within the meaning of the Fifth Amendment because it would amount to a representation that Spencer has the ability to decrypt the devices. See Fisher, 425 U.S. at 410. Such a statement would potentially be incriminating because having that ability makes it more likely that Spencer encrypted the devices, which in turn makes it more likely that he himself put the sought-after material on the devices.

The next question is whether the foregone conclusion rule applies. There is some confusion in the case law regarding what exactly the relevant "foregone conclusion" must be where the government seeks decryption of hard drives. The Eleventh Circuit has held that the government must show that it is a foregone conclusion not only that the defendant has the ability to decrypt the device(s), but also that certain files are on the device(s). In re Grand Jury Subpoena, 670 F.3d at 1347. The In re Grand Jury Subpoena court denied the government's attempt to compel the defendant to decrypt the device at issue in that case because it " 'ha[d] not shown that it had any prior knowledge of either the existence or the whereabouts of the [files]' " on the device. Id. (alterations in original).

***3** The Eleventh Circuit was relying on precedent in which the government requested specific documents from a defendant pursuant to subpoena. See Fisher, 425 U.S. at 410. In Fisher, "Compliance with the subpoena tacitly concede[d] the existence of the papers demanded and their possession or control" by the defendant. Id. Not so in cases like the one at hand, in which the government seeks entire hard drives. Turning over the decrypted devices would not be tantamount to an admission that specific files, or any files for that matter, are stored on the devices, because the government has not asked for any specific files. Accordingly, the government need only show it is a foregone conclusion that Spencer has the ability to decrypt the devices.[2] That the government may have

[1] See Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (stating in dicta that compelling someone to reveal the combination to his wall safe is testimonial for purposes of the Fifth Amendment); Wayne R. LaFave et al., 3 Criminal Procedure § 8.13(a) (4th ed. 2017) ("[R]equiring the subpoenaed party to reveal a passcode that would allow [the government] to perform the decryption...would require a testimonial communication standing apart from the act of production, and therefore make unavailable the foregone conclusion doctrine."); accord, United States v. Kirschner, 823 F. Supp. 2d 665, 668-69 (E.D. Mich. 2010); In re Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *3-4 (D. Vt. Nov. 29, 2007), overruled in part on other grounds, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); Com. Of Virginia v. Baust, No. CR14-1439, 2014 WL 6709960, at *3.

[2] See Orin Kerr, Fifth Amendment protects passcode on smartphones, court holds, Wash. Post (Sept. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/24/fifth-amendment-protects-passcode-on-smartphones-court-holds/?noredirect=on&utm_term=.92228f257a5d ("The details of what records are on the phone should be irrelevant to whether the foregone conclusion doctrine applies because access to the phone is independent of what records are stored inside it. Handing over the passcode has the same testimonial aspect regardless of what is on the phone."); Apple MacPro Computer, 851 F.3d at 248 n.7; In re Search of a Residence in Aptos, Calif. 95003, 2018 WL 1400401, at *6 n.10.

access to more materials where it seeks a hard drive through a search warrant than it would have had if it sought specific files through subpoena is simply a matter of the legal tool the government uses to seek access. To the extent Spencer contends that the government has not adequately identified the files it seeks, that is an issue properly raised under the Fourth Amendment, not the Fifth.

The only remaining question insofar as the applicable legal framework goes is what standard the Court must apply in evaluating whether Spencer's knowledge of the passwords is a "foregone conclusion." In the context of requests for specific documents, the government is required to establish independent knowledge "of the existence, possession, and authenticity of subpoenaed documents with 'reasonable particularity' before the communication inherent in the act of production can be considered a foregone conclusion." United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999), aff'd, 530 U.S. 27 (2000). The "reasonable particularity" standard appears to have been derived from the standard courts use to evaluate whether a warrant is sufficiently specific under the Fourth Amendment. See Stanford v. State of Tex., 379 U.S. 476, 485 (1965).

Courts have continued to apply that standard to cases involving compelled decryption under the Fifth Amendment. See, e.g., In re Grand Jury Subpoena, 670 F.3d at 1349; Apple MacPro Computer, 851 F.3d at 247. But it is nonsensical to ask whether the government has established with "reasonable particularity" that the defendant is able to decrypt a device. While physical evidence may be described with more or less specificity with respect to both appearance and location, a defendant's ability to decrypt is not subject to the same sliding scale. He is either able to do so, or he is not. Accordingly, the reasonable particularity standard cannot apply to a defendant's ability to decrypt a device. (In any event, "reasonable particularity" is not really an evidentiary standard at all. It is better viewed as a substantive standard that helps to ensure that any testimony at issue really is a "foregone conclusion.")

The appropriate standard is instead clear and convincing evidence. This places a high burden on the government to demonstrate that the defendant's ability to decrypt the device at issue is a foregone conclusion. But a high burden is appropriate given that the "foregone conclusion" rule is an exception to the Fifth Amendment's otherwise jealous protection of the privilege against giving self-incriminating testimony. See Fisher, 425 U.S. at 429 (Brennan, J., concurring).

III. DISCUSSION

The question, accordingly, is whether the government has shown by clear and convincing evidence that Spencer's ability to decrypt the three devices is a foregone conclusion. It has. All three devices were found in Spencer's residence. Spencer has conceded that he owns the phone and laptop, and has provided the login passwords to both. Moreover, he has conceded that he purchased and encrypted an external hard drive matching the description of the one found by the government. This is sufficient for the government to meet its evidentiary burden. The government may therefore compel Spencer to decrypt the devices. Once Spencer decrypts the devices, however, the government may not make direct use of the evidence that he has done so. See Robert P. Mosteller, Simplifying Subpoena Law: Taking the Fifth Amendment Seriously, 73 Va. L. Rev. 1, 110 n.108 (1987). If it really is a foregone conclusion that he has the ability to do so, such that his decryption of the device is not testimonial, then the government of course should have no use for evidence of the act of production itself.

***4** Spencer also contends that the magistrate judge erred in holding that the government properly relies on the All Writs Act, 28 U.S.C. § 1651, to compel Spencer to decrypt the devices at issue. She did not. Spencer is "not 'far removed from the underlying controversy' "; compliance " 'require[s] minimal effort' "; and without Spencer's assistance, " 'there is no conceivable way in which the [search warrant] authorized by the District Court could [be] successfully accomplished.' " See Apple MacPro Computer, 851 F.3d at 246 (quoting United States v. New York Tel. Co., 434 U.S. 159, 174–75 (1977)) (alterations in original).

IV. CONCLUSION

The magistrate judge's order was correct in all respects. The motion for relief is **DENIED**.

IT IS SO ORDERED.

Dated: April 26, 2018 CHARLES R. BREYER

United States District Judge