UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF A RESIDENCE IN APTOS, CALIFORNIA 95003

Case No.17-mj-70656-JSC-1

ORDER GRANTING APPLICATION UNDER THE ALL WRITS ACT COMPELLING MICHAEL SPENCER TO AID IN THE EXECUTION OF A SEARCH WARRANT

Re: Dkt. No. 4

On April 26, 2017, this Court authorized a search warrant of a residence believed to be inhabited by Real Party in Interest Ryan Michael Spencer. (Dkt. No. 1.) The warrant authorized the FBI to search the premises and any computers, storage media, routers, modems, and network equipment contained therein, as well as Mr. Spencer himself, for evidence of child pornography. (Dkt. No. 1 at 29-33.[1]) During the search, the FBI seized 12 electronic media items, some of which have been determined to contain child pornography; however, several of the devices are encrypted in whole or in part. (Dkt. No. 10 at ¶¶ 2, 5, 7.) The United States now seeks an order under the All Writs Act, 28 U.S.C. § 1651, compelling Mr. Spencer to decrypt three of these devices: (1) an iPhone 7, Model A1660, serial number F72SDRNGHG7; (2) a Transcend 1TB external hard drive, serial number C842472715; and (3) an Alienware laptop, Model P4sF, serial number 451PM32. (Dkt. No. 4.)

Having considered the parties' briefs and the relevant legal authority, and having had the benefit of oral argument on March 1, 2018, the Court GRANTS the application and orders Mr.

[1] Record citations are to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of the documents.

Spencer to assist in the execution of the search warrant. In doing so, the Court finds that the testimonial value of decryption as to each at-issue device is a "foregone conclusion" such that Mr. Spencer's Fifth Amendment privilege against self-incrimination is not reached.

BACKGROUND

A. Search of Codefendant Petersen's Residence

In April 2017, this Court issued a warrant authorizing the search of Bryan Petersen's residence in Tiburon, California upon a finding of probable cause that he possessed child pornography. The FBI executed that warrant on April 26, 2017. (Dkt. No. 12 at 24, ¶ 3.) In an interview, Petersen admitted to possessing and producing child pornography, and to exchanging child pornography with individuals on the internet. (*Id.* at ¶¶ 3-6.) He identified Spencer as one such individual. (*Id.* at ¶ 3.) Petersen claimed Spencer had surreptitiously photographed naked children in the course of employment as a babysitter. (*Id.* at ¶ 4.) He further admitted to ordering an external hard drive on Amazon.com for delivery to Spencer, who upon receipt filled the drive with "between 10,000 and 100,000" photo/video files of child pornography. (*Id.* at ¶ 3.) Petersen then travelled to Aptos, California to retrieve the drive directly from Spencer. (*Id.*)

Additionally, Petersen gave the FBI passwords to access his electronic devices.[2] (*Id.* at ¶ 6.) The FBI examined Kik messages on Petersen's iPhone, exchanged by Petersen and Spencer in April 2017, and concluded that each had "actively solicited" babysitting jobs in order to take photos of naked children and to share those photos with each other.[3] (*Id.* at 25, ¶¶ 7-8.) These messages contained child pornography sent by both Petersen and Spencer. (*Id.*; 19 at ¶ 9.)

B. Search of Defendant Spencer's Residence

Later that same day, the Court authorized a warrant to search Spencer's residence in Aptos, California. The FBI executed it, with Spencer present, on the morning of April 27, 2017. (Dkt.

[2] Devices seized from Petersen are not at issue.

[3] Kik is a free messaging application. Registered users can exchange texts, photos, and videos.

No. 12 at 25, ¶ 9.) The FBI seized twelve devices in total. (Dkt. No. 10 at ¶ 2.) Among those devices so seized, three are at-issue in this Order. (Dkt. No. 4 at 6-7.)

1. iPhone 7, Model A1660, Serial Number F72SDRNGHG7

The iPhone was in Spencer's hand when the FBI entered his home to execute the search warrant. (*Id.* at 26, ¶ 9.) He admitted ownership and has since produced the password to bypass the iPhone's lock screen. (*Id.*) Reviewing the iPhone, the FBI found Kik messages containing the same child pornography discovered on Petersen's phone. (*Id.* at 19, ¶ 9.) The iPhone also contains a "Spy Camera" application, allowing the user to take surreptitious photographs. (*Id.* at 28, ¶ 21.) Further, the FBI discovered a password-protected application entitled "Secret Folder & Video Vault Pro" ("Secret Folder"). (*Id.* at 19, ¶¶ 10-11.) This application requires 20MB to install but currently occupies 20G of phone memory. (*Id.*) The FBI has linked several files to the application, including "info.e2uapp.photosafe." (*Id.*)

2. Alienware Laptop, Model P4sF, Serial Number 451PM32

This laptop was seized from Spencer's desk and he admitted ownership. (Dkt. No. 12 at 26, ¶ 9.) As with the iPhone, he produced the password to bypass the laptop's lock screen. (*Id.*) However, part of the laptop remains locked under VeraCrypt-brand encryption. (*Id.* at 18-19, ¶ 7.) The government has determined that VeraCrypt does not incorporate a developer backdoor. (*Id.* at 20, ¶ 13.) VeraCrypt's public posture is that it "will never implement [a developer backdoor] even if asked to do so by a government agency."[4] (*Id.*)

At oral argument on March 1, 2018, the government disclosed that, as with the iPhone, it has found child pornography on the unencrypted portion of the Alienware laptop.

3. Transcend 1TB External Hard Drive, Serial Number C842472715

This external hard drive was also seized from Spencer's desk. (*Id.* at 26, ¶ 9.) The FBI has tried and failed to bypass the VeraCrypt software installed on the drive. (*Id.* at 16-17, ¶ 6.) Forensic examination revealed that the drive contains over 900GB of data. (*Id.*)

//

[4] VeraCrypt's position statement is available at https://www.veracrypt.fr/en/FAQ.html.

C. Criminal Charges and Petersen's Plea Bargain

In May 2017, Petersen and Spencer were charged under 18 U.S.C. § 2252(a)(2) with conspiracy to distribute and receive child pornography, distribution of child pornography, receipt of child pornography, and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B).[5] Petersen entered into a plea bargain and pled guilty.[6] In September 2017, Petersen proffered a declaration memorializing his knowledge of Spencer's practices regarding the production, storage, and encryption of child pornography on the at-issue devices. (*Id.*)

D. Declaration of Bryan Petersen

Petersen attests that he met Spencer online in 2011, and that around two years later they began exchanging child pornography, mainly through Kik and Gmail. (Dkt. No. 5 at ¶¶ 1-3.) Eventually, they began taking naked photos of children with whom they worked as babysitters. (*Id.*) Moreover, Spencer confided to Petersen that he had molested children under his care, including one victim who was routinely under the influence of autism medication and unable to wake when touched. (*Id.* at ¶ 6.) Spencer sent photos depicting these attacks as they unfolded. (*Id.* at ¶ 7.) He also recommended to Petersen an aftermarket iPhone camera application allowing the user to photograph subjects surreptitiously. (*Id.* at ¶ 5.)

In particular, Spencer described to Petersen his practice concerning the production, storage, and encryption of child pornography. (*Id.*) First, Spencer "[stood] with the phone close to his body such that no one could see the screen" and then used the iPhone's volume buttons to take a photo. (*Id.* at ¶ 4.) His surreptitious-use application rendered the screen black and ameliorated the risk of discovery as Spencer took pictures of naked children. (*Id.* at ¶ 5.) Second, Spencer saved the photos in a password-protected iPhone application. (*Id.* at ¶ 8.) Third, Spencer transferred the child pornography from the password-protected iPhone application to an encrypted external hard

[5] *United States v. Petersen et al.*, No. 17-cr-259-CRB (N.D. Cal.).

[6] *See* No. 17-cr-259-CRB (Dkt. No. 50, Plea Agreement as to Bryan Petersen.) Under the July 2017 agreement, Petersen pled guilty to violations of: 18 U.S.C. § 2252(a)(2) and (b)(1) (conspiracy to distribute/receive child pornography); 18 U.S.C. § 2251(a) (production of child pornography); 18 U.S.C. § 2252(a)(2) (distribution of child pornography); 18 U.S.C. § 2252(a)(2) (receipt of child pornography); and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography).

drive. (*Id.*) In addition, Spencer described the use of an "encrypted partition" on his laptop used to store child pornography, mentioning an occasion when he brought this laptop to school and nearly "projected child pornography in a classroom." (*Id.* at ¶ 9.)

In January 2016, Spencer told Petersen he planned to buy a new external hard drive with enough space to contain his "very large" collection of child pornography. (*Id.* at ¶ 10.) Spencer further intimated that his collection was stored on "numerous devices...including an encrypted part of his laptop, at least one external hard drive, and his phone." (*Id.*)

In February 2016, Spencer offered to fill an external hard drive with child pornography and to encrypt that drive for Petersen's use, with the condition that Petersen provide the drive. (*Id.* at ¶ 11.) In the following month, Spencer obtained for himself a new external hard drive where he began to store child pornography. (*Id.* at ¶ 12.) He also renewed his prior offer to fill an encrypted external hard drive with child pornography for Petersen. (*Id.*)

Shortly thereafter, Petersen told Spencer that he was shipping him a "Transcend Military Drop Tested 1 TB external hard drive" directly from Amazon.com. (*Id.* at ¶ 13.) Spencer replied that he owned "exactly the same make and model of external hard drive, which was the hard drive to which he was transferring his collection of child pornography." (*Id.*)

Petersen then travelled to Aptos in late 2016 to retrieve the drive from Spencer. (*Id.* at ¶ 14.) Spencer then gave Petersen the Transcend external drive containing child pornography, demonstrating that it was encrypted with VeraCrypt and providing the password. (*Id.*) Spencer next demonstrated how to access encrypted child pornography using the password he had selected for Petersen, which incorporated the name of a child whom Petersen babysat. (*Id.*)

During that Aptos meeting, Petersen saw Spencer connect his iPhone to a "black laptop" and remark that he was transferring "files" from his iPhone. (*Id.* at ¶ 15.) While Petersen watched, Spencer plugged *his* Transcend external drive into the laptop, inputting from memory his VeraCrypt password in order to access child pornography. (*Id.* at ¶ 16.) In so doing, Spencer navigated through the black laptop to his Transcend external hard drive and accessed child pornography. (*Id.*) Petersen also saw Spencer download child pornography from a website called "Boytraders" onto the Transcend external drive. (*Id.* at ¶ 17.)

Several days later, Spencer asked Petersen whether he had memorized the VeraCrypt password and Petersen replied that he had. (*Id.* at ¶ 18.) Spencer noted that his VeraCrypt password was easy to recall because it incorporated "the name of a boy for whom he claimed to have feelings," much like the password he prepared for Petersen. (*Id.*) Sometime thereafter, Spencer told Petersen the hard drive he had received in Aptos contained "one-quarter to one-third" of his total child pornography collection. (*Id.* at ¶ 19.)

E. Recovery of Additional Kik Messages

The FBI used digital tools to recover additional Kik messages dating from January 2016 to November 2016. (Dkt. No. 12 at 26-28.) In these messages, Spencer offers detailed descriptions of his practices regarding child pornography collection and storage.

In January 2016, Spencer mentioned his "300 [gigabyte]" child pornography collection, remarking that he needed a new external hard drive to store it. (Dkt. No. 12 at 26, ¶ 12.) The following month, Spencer sent child pornography to Petersen, characterizing those images as a "fraction" of his total collection. In addition, Spencer said that his child pornography was stored on: "An external drive. Encrypted up the ass. That you can smash with a hammer at a moment's notice." (*Id.* at ¶ 13.) Spencer noted that he could "very easily" set up an encrypted external drive for Petersen. (*Id.*) In another message, Spencer opined that in addition to his hard drive, his computer "might be incriminating too." (*Id.*) He also messaged Petersen that he had recently had sex with a 15-year-old boy and had "so many pics I have to download on my computer lol." (*Id.* at ¶ 14.)

In March 2016, Spencer indicated to Petersen that he had acquired a new 1TB external hard drive that he was "encrypting...and making [] his bitch." (*Id.* at 27, ¶ 15.) He then offered to create for Petersen a "computer vault" for storing child pornography. (*Id.*) Spencer messaged: "I can make you one if you send me a hard drive. You can destroy it with a hammer and all files really gone. Takes under a minute. Accessed externally to computers." (*Id.*) In another message Petersen asked whether Spencer felt guilty about their actions. (*Id.*) Spencer responded that he did not feel "bad or anything" but did allow that he was "worried legally speaking." (*Id.*)

The next day, Petersen sent a picture of the hard drive he planned to buy—a "Transcend Military Drop Texted 1TB external hard drive." (*Id.* at ¶ 16.) Spencer replied: "I hav [sic] that exact one….[t]hat's the one I got." (*Id.*) He reiterated his previous offer to create for Petersen a "computer vault"—an encrypted external hard drive storing child pornography. (*Id.* at ¶ 15.)

In October 2016, Kik messages show Petersen and Spencer arranging a time to meet in person for Petersen to retrieve the promised hard drive. (*Id.* at ¶ 18.) Spencer suggested Petersen arrive early so they would have enough time to "check out the collection." (*Id.*) Moreover, Spencer indicated that he would soon upload child pornography "from [his] drive to Dropbox," and that "[t]he stuff on my computer is hot as fuck." (*Id.*)

In November 2016, Spencer messaged that he had a babysitting job for the weekend. He also observed to Petersen that he could "control and take pictures from [his] iPhone" using his watch. (*Id.* at ¶ 19.) He was thus able to photograph children from another room if he "propped up" his iPhone for vantage. (*Id.*) Spencer recommended this application to Petersen. (*Id.*)

Additional messages recovered by the FBI depict Spencer educating Petersen on how to use encryption on the external hard drive. (*Id.* at 28, ¶ 20.) Spencer explained that to access the encrypted drive from a computer, Petersen needed to "install Veracrypt on the pc." (*Id.*) But to send files from the external drive, Spencer instructed that Petersen must "download 7z on his computer and throw it into a zipped file with a password....[t]hen you can upload it direct to the web and send the zip file. If it's encrypted then people can't fuck with it." (*Id.*) Spencer explained that Petersen could send files directly from the encrypted drive: "[w]hen you mount it with Veracrypt it decrypts the files, when you dismount it they re-encrypt." (*Id.*)

F. Prior Warrant Extensions and Failed FBI Decryption Efforts

The government has requested and received two good-cause warrant extensions in light of the challenge presented by Mr. Spencer's encryption. Magistrate Judge Laporte granted the first extension on August 11, 2017 and the second on December 11, 2017. (Dkt. Nos. 2, 9, 11.) The government investigation and bypass efforts are memorialized in the declarations of FBI Special Agents Hadley and Marceau.[7] (Dkt. No. 12 at 15, 23.)

On October 25, 2017, the government filed the underlying application under the All Writs Act, 28 U.S.C. § 1651, to compel Mr. Spencer to produce in a fully unlocked state the iPhone, Alienware laptop, and Transcend 1TB external hard drive. (Dkt. No. 4.) After several stipulated extensions, Mr. Spencer filed an opposition brief and the government a reply. (Dkt. No. 12 & 14.) The Court heard oral argument on March 1, 2018. (Dkt. No. 18.)

DISCUSSION

The question here is whether compelling Mr. Spencer under the All Writs Act to decrypt these devices constitutes a violation of his Fifth Amendment privilege, or whether, as the government maintains, any testimonial value inhering to the act of decryption is a foregone conclusion.[8] The Court finds that the foregone conclusion doctrine applies, as set forth below. The record demonstrates that Mr. Spencer's knowledge of the encryption passwords is a foregone conclusion and—in addition—that the authenticity, possession, and existence of the sought-after files are a foregone conclusion. In either event, the testimony inhering to the act of decryption is a foregone conclusion that "adds little or nothing to the sum total of the Government's information." *Fisher v. United States*, 425 U.S. 391, 411 (1976).

//

//

[7] Agent Hadley worked the Petersen and Spencer investigations. She interviewed Petersen and assisted in the search of Spencer's residence. Agent Marceau, a Digital Evidence Extraction Technician, assisted in the search of Spencer's residence and the FBI's subsequent bypass efforts. Agent Marceau said of Spencer's encryption: "if the FBI could execute a brute force attack with a guess rate of 1,000,000 passwords per second, it would take more than 1,649,859 years to enter every conceivable combination [of 11-digit password]." (Dkt. No. 12. at 21, ¶ 18.)

[8] Mr. Spencer conceded at oral argument that the All Writs Act is the appropriate vehicle to compel decryption. *See* 28 U.S.C. § 1651; *United States. v. New York Telephone Co.*, 434 U.S. 159, 174-175 (1977) (articulating test for All Writs Act application); *United States v. Apple MacPro Computer*, 851 F.3d 238, 246 (3d Cir. 2017) (no plain error where the magistrate judge applied *New York Telephone* and compelled defendant to decrypt); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012) (same, but applying preponderance standard).

A. The Fifth Amendment Privilege

The Fifth Amendment provides that "[n]o person…shall be compelled in any criminal case to be a witness against himself." But "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence." *Fisher*, 425 U.S. at 408. "[T]he privilege protects a person only against being incriminated by his own compelled testimonial communications." *Id*. at 409. It encompasses incriminating answers as well as those "furnish[ing] a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hoffman v. United States*, 341 U.S. 479, 486 (1951). The privilege may also encompass the very act of production if that act "implicitly communicate[s] statements of fact." *See Fisher*, 425 U.S. at 410; *United States v. Hubbell*, 530 U.S. 27, 36 (2000). The government concedes here that compelling decryption of the potentially incriminating contents of the at-issue devices would—absent a further showing on its part—implicate the Fifth Amendment. And the government has not sought a grant of immunity for Mr. Spencer.[9] However, as set forth below, "no Fifth Amendment right is touched" because any testimony inhering to Mr. Spencer's compelled act of decryption is a foregone conclusion. *In re Grand Jury Subpoena, Dated Apr. 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004) ("*Doe I*") (citing *Fisher*, 425 U.S. at 411).

B. The Foregone Conclusion Doctrine Applies

The Court turns next to the critical question: whether the testimony inhering to Mr. Spencer's act of production is a foregone conclusion such that ordering him to decrypt the at-issue devices will not implicate the Fifth Amendment. The foregone conclusion doctrine is an application of the Fifth Amendment "by which the Government can show that no testimony is at issue." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1343 n.19 (11th Cir. 2012). The Supreme Court articulated the foregone conclusion doctrine in *Fisher v.*

[9] Because the foregone conclusion doctrine applies, this Order does not reach the question of immunity. *See, e.g., United States v. Hubbell*, 530 U.S. 27, 45-46 (2000) (production could not be compelled absent sufficient grant of immunity where foregone conclusion doctrine inapplicable); *United States v. Doe*, 465 U.S. 605, 617 (1984) ("*Doe II*") ("to satisfy…the Fifth Amendment, a grant of immunity need be only as broad as the privilege against self-incrimination")

United States, where it upheld the subpoena of potentially incriminating tax documents because the government did not rely on the respondent's tacit testimony—that is, the "truth-telling" arising from the very act of production—to prove the existence of the documents or that the respondent possessed them. *Fisher*, 425 U.S. at 410-11. The Court thus held that "[t]he existence and location of the papers [were] a foregone conclusion and the taxpayer add[ed] little or nothing to the sum total of the Government's information." *Id.* ("doubtful that implicitly admitting the existence and possession of the papers [rose] to the level of testimony within the protection of the Fifth Amendment"). Because the implicit testimony was a foregone conclusion, the matter reduced to a question "not of testimony but of surrender." *Id.*

The question of the foregone conclusion doctrine's application in the context of compelled decryption presents a question of first impression to the Ninth Circuit. After considering the parties' submissions, surveying the relevant legal authority, and having had the benefit of oral argument, the Court finds that the foregone conclusion doctrine applies to each at-issue device.

1. The Court can Order Mr. Spencer to Decrypt Each Device as it is a Foregone Conclusion That he Knows the Encryption Passwords to do so

The Court finds that the testimony inhering to the act of decryption is that Mr. Spencer knows the encryption password. The act of decryption requires nothing more.[10] Accordingly, the

[10] The foregone conclusion doctrine most often arises with regard to *document subpoenas* and accordingly, precedent reflects concerns unique to that context. *See, e.g.*, *Fisher*, 425 U.S. at 411 (articulating doctrine as to summonsed tax documents); *Hubbell*, 530 U.S. at 41 (broad subpoena of documents the "functional equivalent" of answering "detailed written interrogatory or a series of oral questions"); *Doe I*, 383 F.3d at 911 (subpoena "which seeks all documents within a category but fails to describe those documents with any specificity indicates that the government needs the act of production to build its case"). But the *compelled decryption* of lawfully-seized devices does not present identical concerns. As a practical matter, a respondent can know a password—and can thus decrypt the device or program to which the password is linked—without ownership, possession, or even general knowledge of files ultimately discovered. Thus where, as here, the *contents* of the encrypted devices are not alleged to be privileged, the government need only demonstrate sufficient prior knowledge that the defendant knows the password to the encrypted device or program at-issue. *Fisher*, 425 U.S. at 410 (inquiry into elements of incrimination and implied testimony "do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof"); *Apple MacPro Computer*, 851 F.3d at 248 (upholding decryption order under plain error review as "*any* testimonial aspects of [the act of decryption] were a foregone conclusion") (emphasis added).

Court holds that if the respondent's knowledge of the relevant encryption passwords is a foregone conclusion, then the Court may compel decryption under the foregone conclusion doctrine. *See United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3d Cir. 2017) ("a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony…implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is "*I, John Doe, know the password for these devices*") (emphasis added). Further, "[t]he government bears the burden of proof and must have had the requisite knowledge before issuing the summons or subpoena." *See Bright*, 596 F.3d at 692. Finally, the government's showing of independent knowledge must be made to the standard of "reasonable particularity." *See Doe I*, 383 F.3d at 909; *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1202 (9th Cir. 2013). The Court finds that the government has shown with reasonable particularity that Mr. Spencer knows the encryption passwords responsive to each at-issue device such that he can produce them in a fully-decrypted state. The Court first considers the at-issue iPhone and its "Secret Folder" application and then turns to the Alienware laptop and the Transcend 1TB external hard drive.

a. iPhone 7, Model A1660

First, it is a foregone conclusion that Mr. Spencer knows the password to fully decrypt the at-issue iPhone 7, inclusive of the encrypted "Secret Folder" application, such that he can produce the phone in a fully-unlocked state. (Dkt. No. 12 at 19.) Spencer admitted ownership of the phone and has provided—through counsel—the passcode to bypass its lock screen. (*Id*. at 26, ¶ 9.) This scenario arose in *Apple MacPro Computer* where the defendant "provided the password to access [an at-issue iPhone 6 Plus] but did not grant access to an application...which contained additional encrypted information." *See Apple MacPro Computer*, 851 F.3d at 243 (reviewing application of foregone conclusion doctrine under plain error standard in lieu of reasonable particularity as defendant failed to preserve objection). Because the defendant "had opened [the iPhone] for the police by entering a password," it was not plain error to find that he could similarly access the *secondary* encrypted application within the same phone. *Id*. at 248 (affirming application of foregone conclusion doctrine). Whereas in *Apple MacPro*, the *primary* grant of access was sufficient to impute sufficient knowledge of a *secondary* password, here the government has the same primary grant of access but has even greater independent knowledge as to the secondary application. *Id*. at 247-48. In particular, Petersen credibly attests that Spencer described his routine use of a password-protected iPhone application to store child pornography.[11] (Dkt. No. 5. at 2, ¶ 8.) Finally, even as the government bears the burden of production, the Court notes that Mr. Spencer does not dispute his ability to access the "Secret Folder" application. Nor does Mr. Spencer dispute knowledge of the encryption passwords as to any device, or his ownership more generally. In light of the foregoing, the government has shown with reasonable particularity that it is a foregone conclusion that Mr. Spencer knows the password such that he can fully-decrypt the at-issue iPhone 7, inclusive of the "Secret Folder" application. *Doe I*, 383 F.3d at 909; *Apple MacPro Computer*, 851 F.3d at 243.

b. Alienware Laptop, Model P4sF

Second, it is a foregone conclusion that Mr. Spencer knows the VeraCrypt password such that he can produce the Alienware laptop in a fully-unlocked state. He admitted ownership and—as with the iPhone—he furnished a passcode allowing the government to access part of the laptop, but not the portions encrypted with VeraCrypt which are implicated here. (Dkt. No. 12. at 26, ¶ 9). Moreover, Petersen attests that Spencer spoke of storing child pornography in an encrypted laptop partition—even mentioning an incident at school where he had very nearly "projected child pornography in a classroom" from that laptop. (Dkt. No. 5 at 2-3, ¶ 9.) In *United States v. Fricosu*, the government carried its burden of showing "that [respondent] was [the laptop's] sole or primary user, who, in any event, [could] access the encrypted contents" where the respondent admitted in a recorded telephone call, and later confirmed, that sought-after files were located on her password-protected laptop. *United States v. Fricosu*, 841 F. Supp. 2d 1235-37 (D. Colo. 2012) (applying foregone conclusion doctrine under preponderance standard in lieu of reasonable

[11] Petersen also claimed that Spencer used a surreptitious camera application to photograph naked children. (Dkt. No. 5 at 2, ¶ 5.) The Court finds that assertion credible. Spencer's November 2016 Kik messages—independently recovered by the FBI—show that he discussed using a surreptitious camera application. (Dkt. No. 12 at 27, ¶ 19.) The FBI also discovered a "Spy Camera" application installed on Mr. Spencer's phone that allowed the user to take surreptitious photographs. (*Id*. at 28, ¶ 21.)

particularity). Of *three* laptops seized prior to the respondent's admission, only *one* laptop fit the description and the court applied the foregone conclusion doctrine, thus compelling decryption. *Id*. at 1237. Here the government has even more independent knowledge. First, Petersen saw Spencer enter a password from memory to access VeraCrypt on a "black laptop." (Dkt. No. 5 at 3, ¶ 15.) Second, the Alienware laptop is partially encrypted with VeraCrypt and is the *only* functioning laptop seized. (Dkt. No. 12 at 16, ¶ 5; 18-19, ¶ 7.) Further, Petersen attests that Spencer not only instructed him in the use of VeraCrypt but later said of his password-selection protocol: "[Spencer] had made his encryption password easier to remember by incorporating the name of a boy for whom he claimed to have feelings, in a format similar to the encryption password he had created for me."[12] (Dkt. No. 5 at 3-4, ¶¶ 14, 16.) Accordingly, the government has shown with reasonable particularity that it is a foregone conclusion that Mr. Spencer knows the password such that he can fully-decrypt the at-issue the Alienware laptop, inclusive of VeraCrypt. *Doe I*, 383 F.3d at 909; *Fricosu*, 841 F. Supp. 2d at 1237.

c. Transcend 1TB External Hard Drive

Third, it is a foregone conclusion that Mr. Spencer knows the VeraCrypt password such that he can produce the Transcend 1TB external hard drive in a fully-unlocked state. This device was seized from the same desk as the Alienware laptop. (Dkt. No. 12 at 26, ¶ 9.) Later, during their Aptos meeting, Petersen saw Spencer enter the VeraCrypt password from memory to access this device. (Dkt. No. 5 at ¶¶ 15-17.) Here, messages recovered by the government show that Spencer said he: (1) owned a Transcend 1TB external hard drive "exact[ly]" like Petersen's; (2) that he used encryption on his external hard drive; and (3) that he used VeraCrypt. (Dkt. No. 12 at 28, ¶¶ 15-16, 20.) Only one seized device meets these criteria: the Transcend external hard drive seized by the FBI from Spencer's desk, which was the only such device seized from Spencer. *See Fricosu*, 841 F. Supp. 2d at 1235-37 (as respondent admitted the files were on encrypted laptop and only one of three seized both matched that admission and had nominal indica of ownership, it

[12] The Court finds Petersen's statements as to both Transcend drives credible. Petersen immediately furnished his passwords to the FBI. (Dkt. No. 12 at 24, ¶ 6.) The FBI discovered—on *Spencer's* Alienware laptop—the VeraCrypt password to access *Petersen's* identical Transcend hard drive, thereby corroborating Petersen's earlier statements. (Dkt. No. 12 at 19, ¶ 8.)

was a foregone conclusion that "[respondent] was [the] sole or primary user, who, in any event, [could] access the encrypted [files]"). Accordingly, the government has shown with reasonable particularity that it is a foregone conclusion that Mr. Spencer knows the password such that he can fully-decrypt the Transcend external hard drive, inclusive of VeraCrypt. *Id.*; *Doe I*, 383 F.3d at 909.

Because the act of decryption impliedly testifies only as to the knowledge of passwords, and Mr. Spencer's knowledge of the passwords as to each at-issue device is a foregone conclusion, the Court could grant the government's motion on this basis. But as this issue presents a question of first impression in the Ninth Circuit, the Court also considers whether the foregone conclusion doctrine applies under the analysis applied to the traditional document-subpoena inquiry.

2. The Court can Order Mr. Spencer to Decrypt Each Device as it is a Foregone Conclusion That the Encrypted Child Pornography: (1) Exists; (2) is Authentic; and (3) was Possessed or Owned, and Accessed by Mr. Spencer

"When the existence and location of the documents…are a foregone conclusion and the witness adds little or nothing to the sum total of the Government's information by conceding that he in fact has the [documents], then no Fifth Amendment right is touched because the question is not of testimony but of surrender." *Doe* I, 383 F.3d at 910 (citing *Fisher*, 425 U.S. at 411). Under this analysis, the government must establish its independent knowledge of three elements: the files' existence, the files' authenticity, and respondent's possession or control of the files.[13] *Bright*, 596 F.3d at 692; *accord Sideman & Bancroft, LLP*, 704 F.3d at 1202; *Apple MacPro Computer*, 851 F.3d at 248-49 (no plain error in decryption order as "any testimonial aspects of [decryption] were a foregone conclusion" where record "amply supported" findings that: "(1) the Government had custody of the devices; (2) prior to the seizure, [respondent] possessed, accessed, and owned all devices; and (3) there [were] images on the electronic devices that constitute[d] child pornography"). Again, the government "bears the burden of proof and must have had the requisite knowledge before issuing the summons or subpoena." *Bright*, 596 F.3d at 692; *accord*

[13] As a basic premise, the Court notes that each seized device "exists" in the corporeal sense as each remains in government custody.

Doe I, 383 F.3d at 909. And its proof must be made with "reasonable particularity." *Sideman & Bancroft, LLP*, 704 F.3d at 1202; *Doe I*, 383 F.3d at 909. As set forth below, the Court finds that the government has shown with at least reasonable particularity—as to each device—that it is a foregone conclusion that: (1) Mr. Spencer owned or possessed each device and thus owned or possessed the encrypted files, and can fully-decrypt each device; (2) that the files exist; and (3) that the files are authentic. The Court looks first to the elements of possession and existence, considering each device in turn, then turns to the question of authenticity.

a. iPhone 7, Model A1660

The Court finds that Mr. Spencer's ownership or possession of the iPhone—and the Secret Folder application therein—are a foregone conclusion. The iPhone was seized from his hand when the FBI commenced to search his residence and he promptly admitted ownership. (Dkt. No. 12, at 26, ¶ 9.) He does not now dispute ownership and has provided through counsel the passcode to bypass the iPhone's lock screen. (*Id.*) Since Mr. Spencer owns and can access the iPhone, he owns and can access the encrypted "Secret Folder" therein. *Apple MacPro Computer*, 851 F.3d at 248. Moreover, Petersen credibly communicated that Spencer described his practice of using a password-protected iPhone application to store child pornography. (Dkt. No. 5. at 2, ¶ 8.) Only one such application was discovered here. *Fricosu*, 841 F. Supp. 2d at 1237. Thus, the government has shown with at least reasonable particularity that Mr. Spencer owns the iPhone and the "Secret Folder" application.

The Court also finds that the existence of child pornography on the iPhone's "Secret Folder" application is a foregone conclusion. First, as an initial matter, the government already discovered child pornography in Spencer's Kik messages on the iPhone more generally. (Dkt. No. 12 at 19, ¶ 9.) Second, as set forth above, Petersen credibly attests that Spencer described his practice of storing child pornography in a password-protected application on his iPhone. (Dkt. No. 5 at 2, ¶ 8.) There was only one iPhone seized, and it contains one such application. (Dkt. No. 12 at 19); *see Fricosu*, 841 F. Supp. 2d at 1237 (existence of files a foregone conclusion where respondent admitted to third party that sought-after files existed on password-protected laptop and only one laptop out of the three seized was password-protected). Third, forensic review showed that the Secret Folder application "exists" on the iPhone; that it requires 20MB to install; and that it now contains more than 20GB of encrypted data. (Dkt. No. 12 at 19 ¶ 9.) The foregone conclusion doctrine—regardless of whether applied to decryption or document production—does not require knowledge of specific file names. *See In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1349 n.28 (11th Cir. 2012). But such knowledge "[is] an easy way for the Government to carry its burden of showing that the existence of the files it seeks is a foregone conclusion." *Id.*; *In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009) (existence a foregone conclusion where, upon initial grant of access to at-issue laptop, border agent saw child pornography and a file entitled "2yo getting raped during diaper change"). Here, the FBI has linked files to the Secret Folder iPhone application, including "info.e2uapp.photosafe." (*Id*. at 19, ¶ 11.)

Mr. Spencer insists the government is attempting to force access to an iPhone folder it knows nothing about. There is no question that a mere showing of encryption cannot prove the element of existence "to any degree of particularity." *See Grand Jury Subpoena*, 670 F.3d at 1347 ("we are not persuaded by the suggestion that simply because the devices were encrypted necessarily means that [the defendant] was trying to hide something"). But here the government has independently shown more. Petersen expressly noted Spencer's mention of a "password-protected iPhone application" used to store child pornography for later transfer to an encrypted hard drive. (Dkt. No. 5 at ¶ 2); *Fricosu*, 841 F. Supp. 2d at 1237. And although Petersen did not claim to have seen Spencer open or display any files on the iPhone when they met in Aptos, he did see Spencer plug in the iPhone and transfer "files" while they were viewing child pornography. (Dkt. No. 5 at 3, ¶ 15.) Thus, the Court finds that the government has shown with at least reasonable particularity that child pornography exists within the iPhone's "Secret Folder" application. *Doe I*, 383 F.3d at 910 (application of the doctrine does not demand "actual knowledge of the existence and location of each and every responsive document").

b. Alienware Laptop, Model P4sF

The Court finds that Spencer's ownership of the Alienware laptop is a foregone conclusion. This laptop was seized from Spencer's desk and he admitted ownership, which he does not now dispute. (Dkt. No. 12. at 26, ¶ 9.) Further, as with his iPhone, Spencer furnished a passcode allowing the government to access other parts of the laptop, but not those portions encrypted with VeraCrypt. (*Id.*) Thus, the Court finds that the government has shown with at least reasonable particularity that Mr. Spencer owns the Alienware laptop.

The Court also finds that the existence of child pornography on the encrypted portions of the Alienware laptop is a foregone conclusion. Petersen attests that Spencer told him of his practice of using an encrypted laptop partition to store child pornography and part of the Alienware laptop is encrypted. (Dkt. No. 5 at 2, ¶ 9) (Dkt. No. 12 at 18, ¶ 7.) Further, Kik messages recovered by the FBI show Spencer claiming that files "on [his] computer [are] hot as fuck" and that his "computer might be incriminating too." (*Id*. at 26-27, ¶ 13, 18.)

Mr. Spencer insists the government cannot meet its burden of showing that child pornography exists on the Alienware laptop because *two* laptops were seized by the FBI—the black-and-silver Alienware implicated here as well as a black Lenovo recovered in a non-functioning state as it had no hard drive—and Petersen did not clearly identify the "black laptop" he saw in Aptos as the at-issue Alienware laptop. The Court is not persuaded. First, only one working laptop was seized. It is partly-encrypted with VeraCrypt, which was Spencer's preferred encryption software (or in any event, is the encryption software installed on two of the three at-issue devices). (Dkt. No. 12 at 28, ¶ 20.) Second, Petersen directly implicates "[Spencer's] laptop." (Dkt. No. 5 at 2, ¶ 9.) Specifically, Petersen watched Spencer access child pornography on a "black laptop." (*Id.*) Third, Spencer's own messages likewise implicate his laptop: (1) claiming the child pornography on it was "hot as fuck" and (2) that the laptop "might be incriminating." (Dkt. No. 12 at 26-28, ¶¶ 13, 15, 18); s*ee Fricosu*, 841 F. Supp. 2d at 1237. In addition, the government disclosed at oral argument that it has since discovered child pornography on the accessible part of the laptop. Thus, the Court finds that the government has shown with at least reasonable particularity that child pornography exists within the VeraCrypt-encrypted drive partitions of the Alienware laptop.

//

//

c. *Transcend 1TB External Hard Drive*

The Court likewise finds that Mr. Spencer's ownership of the Transcend 1TB external hard drive is a foregone conclusion. First, the hard drive was seized from the same desk as the Alienware laptop which Spencer admitted to owning. (Dkt. No. 12 at 26, ¶ 9.) Further, Spencer lived in that room for the preceding five years and no evidence suggests he shared the space. (Dkt. No. 4 at 19:20-22.) Second, Petersen attests that when he sent Spencer a Kik message containing a picture of a Transcend external hard drive he had recently purchased for himself, Spencer replied that he owned "exactly that same make and model of external hard drive." (Dkt. No. 5 at 3, ¶ 13.) Later, at their Aptos meeting, Petersen saw Spencer using the Transcend hard drive. (*Id*. at ¶¶ 15-17.) Finally, the Court notes that Spencer does not now dispute ownership. *Apple MacPro Computer*, 851 F.3d at 248. Accordingly, the Court finds that the government has established with at least reasonable particularity that Mr. Spencer's ownership of the Transcend hard drive is a foregone conclusion.

Lastly, the Court finds that the existence of child pornography on the Transcend hard drive is a foregone conclusion. First, recovered Kik messages from January 2016 show Spencer claiming that he had "like 300 gigabytes" of child pornography and that he needed a new external hard drive to store them. (Dkt. No. 12 at 26 ¶ 12.) At present, the drive contains over 900GB of data. (*Id*. at 17, ¶ 6.) In February 2016, Spencer messaged Petersen that he was storing child pornography on an external drive that was "encrypted up the ass" and could be "smash[ed] with a hammer at a moment's notice." (*Id*. at 26, ¶ 13.) The next month, Spencer messaged that he had recently purchased a new external hard drive that he was "[e]ncrypting...and making [his] bitch." (*Id*. at 27, ¶ 15.) Second, Petersen attests that Spencer showed him child pornography on the Transcend drive when they met in Aptos in late 2016. (Dkt. No. 5 at 3-4, ¶ 16-17.) Mr. Spencer raises no dispute as to the sufficiency of the government's showing at to the Transcend drive. Accordingly, the government has carried its burden of establishing the existence of child pornography on the Transcend drive to the required standard of reasonable particularity. *Bright*, 596 F.3d at 692.

//

d. The Files Sought by the Government are Authentic

The government presumptively carries its burden of authenticity as to the iPhone, Alienware laptop, and Transcend external hard drive. This element requires "that not only must the Government show that it can independently establish that the summonsed documents are what they purport to be, it must demonstrate that it is not compelling the [respondent] to use his discretion in selecting and assembling the responsive documents, and thereby tacitly providing identifying information that is necessary to the government's authentication of the subpoenaed documents."[14] *See Sideman & Bancroft, LLP*, 704 F.3d at 1203; *Doe I*, 383 F.3d at 912 (internal citations omitted). But in compelled decryption cases—such as this—involving *seized devices* the authenticity element is routinely cited but only applied loosely if at all. *Apple MacPro Computer*, 851 F.3d at 247 (citing but not applying authenticity requirement); *Grand Jury Subpoena*, 670 F.3d at 1346 (same); *Fricosu,* 841 F. Supp. 2d at 1237 (rejecting defendant's argument that "hard drive was imaged before it was read...undermined [the device's] validity or authenticity" where government testified to integrity of forensic procedures); *In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009) (act of decryption "not necessary to authenticate [the encrypted device]" where possession was admitted and defendant initially granted access to border agent who observed child pornography on the device at-issue).

In considering the element of authenticity, the Court finds persuasive that Agent Marceau, an FBI Digital Evidence Extraction Technician, attested to his use of "authorized practices and procedures" as to each at-issue device. (*See* Dkt. No. 12 at 15-21.) Moreover, the FBI has already discovered child pornography on the accessible part of iPhone and, at oral argument, disclosed that it had discovered child pornography on the accessible part of Alienware laptop. Accordingly, this Court finds that the government can independently determine whether the at-issue devices, upon full decryption, contain additional child pornography without relying on the "truth-telling" of Mr.

[14] Implicit authentication challenges arise mainly out of document subpoenas. *See, e.g., Hubbell,* 530 U.S. at 41 (compliance with broad subpoena similar to answering detailed interrogatory or oral questioning); *Fisher*, 425 U.S. at 412-13 n.12 ("[t]he "implicit authentication" rationale appears to be the prevailing justification for the Fifth Amendment's application to documentary subpoenas"); *Doe I*, 383 F.3d at 911 (broad category-based document subpoena demonstrated that government relied on act of production to prove its case).

Spencer in order to do so. *Fisher*, 425 U.S. at 411. The authenticity of the files is thus a foregone conclusion. *Bright*, 596 F.3d at 692.

3. *Mr. Spencer's Remaining Arguments Against Decryption are Unavailing*

Mr. Spencer insists compelled decryption amounts to an abrogation of privacy rights. As Mr. Spencer articulates no relevant authority to support that proposition—and indeed, does not challenge the sufficiency of the search warrant underlying these proceedings—the Court is not persuaded. The Supreme Court has made clear that the search of cell phone data requires a search warrant. *See Riley v. California*, 134 S. Ct. 2473, 2485 (2014). Here, the government has sought and obtained such a warrant. (Dkt. No. 1 at 40-43.) Nor does Mr. Spencer insist the encrypted files are *themselves* privileged.[15] Mr. Spencer's general privacy argument is thus unavailing.

Mr. Spencer also insists that the Court errs in according weight to the testimony of an unreliable codefendant. This argument, too, is unconstructed and lacks supportive authority. The foregone conclusion doctrine simply requires that the government point to an independent source of prior knowledge. *Bright*, 596 F.3d at 692. This independent knowledge requirement does not qualify the source of that knowledge, except that it cannot derive from the respondent's own implied testimony. For example, courts have applied the foregone conclusion doctrine to compel decryption where the government's independent knowledge derived from the observations of a defendant's own sister and even from a government agent. *Apple MacPro Computer*, 851 F.3d at 248 (defendant's sister who saw him view child pornography on at-issue device(s) provided important source of independent knowledge); *Boucher*, 2009 WL 424718 at *2 (ICE agent who saw child pornography on at-issue device provided critical source of independent knowledge). Spencer offers no authority, persuasive or otherwise, showing that a source of independent knowledge was rejected (or could be rejected) because it was not independent enough. In any

[15] *See, e.g.*, *Hubbell*, 530 U.S. at 35-36 (it is a "settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not compelled within the meaning of the privilege") (internal quotations omitted); *Doe II*, 465 U.S. at 611-12 (files created absent compulsion "cannot be said to contain compelled testimonial evidence"); *Fisher*, 425 U.S. at 410-11 (we are confident that however incriminating the contents of the accountant's workpapers might be, the act of producing...would not itself involve testimonial self-incrimination").

event, Petersen's testimony is either consistent with what he told the government upon the execution of the search warrant at his home, or corroborated by other evidence, such as Mr. Spencer's Kik messages or the form of the devices seized from Spencer. Petersen's testimony is thus reliable.

Here, the government has made its showing using two independent sources of knowledge: Petersen and Spencer. Petersen's immediate confession implicated Spencer and gave rise to the search warrant underlying this Order. (*See* Dkt. No. 1, Statement of Probable Cause at 14-18.) Later, Petersen pled guilty and entered a cooperation agreement with the government, proffering a declaration in furtherance of the prosecution. (See Dkt. No. 5, Declaration of Bryan Petersen.) And when Spencer provided the passcode to bypass the iPhone's lock screen, the government uncovered inculpatory messages authored by Spencer, listed in relevant part in Section E above. (*See* Dkt. No. 12 at 26-28.) The government satisfies the independent knowledge requirement under any reading of the foregone conclusion doctrine.

***

In sum, the Court finds that the government has satisfied to the standard of reasonable particularity that Mr. Spencer knows the encryption passwords to each at-issue device and that this is sufficient to grant the government's application here. In addition, to the extent necessary, the Court finds the government has satisfied to the standard of reasonable particularity that it has prior independent knowledge as to: (1) Mr. Spencer's ownership or control of each device; and (2) the existence of child pornography within the encrypted devices and/or applications at-issue; and (3) that the files sought are authentic. In either event, the testimony inhering to the act of decryption is a foregone conclusion "add[ing] little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411.

CONCLUSION

For the reasons stated above, the government's application is GRANTED as to: (1) the iPhone 7, Model A1660, serial number F72SDRNGHG7; (2) the Transcend 1TB external hard drive, serial number C842472715; and (3) the Alienware laptop, Model P4sF, serial number 451PM32. Pursuant to the All Writs Act, the Court orders Mr. Spencer to provide the government

United States District Court
Northern District of California

with the encryption passwords for the above devices or to decrypt the devices himself such that the government has access to the devices' files.

Any party may file objections to this Order with Judge Breyer within 14 days after being served with a copy. *See* 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b); Civ. L.R. 72-3. Failure to file an objection may waive the right to review of the issue in the district court.

This Order disposes of Docket No. 4.

IT IS SO ORDERED.

Dated: March 20, 2018

Jacqueline Scott Corley

JACQUELINE SCOTT CORLEY
United States Magistrate Judge