UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

In the Matter of
THE DECRYPTION OF A SEIZED
DATA STORAGE SYSTEM

Case No.: 13-M-449

ORDER DENYING APPLICATION TO COMPEL DECRYPTION

On April 3, 2013, the government applied under the All Writs Act, 28 U.S.C. § 1651,[1] for an order compelling Jeffrey Feldman ("Feldman") to "assist in the execution of a federal search warrant by providing federal law enforcement agents a decrypted version of the contents of his encrypted data storage system, previously seized and authorized for search under a federal search warrant."[2] (App. at 12.) The primary issue presented by the government's application is whether compliance with such an order would involve incriminating testimony within the protection of the Fifth Amendment.

I. FACTS

FBI Special Agent Brett Banner ("Banner") submitted an affidavit in support of the government's application, which stated the following facts. On January 22, 2013, a warrant was issued,

[1] "The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985). The Supreme Court has applied the Act to, for example, "persons who . . . are in a position to frustrate the implementation of a court order or the proper administration of justice." *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174 (1977) (upholding an order compelling a telephone company to provide assistance necessary to implement a pen register).

[2] The previously issued search warrant is filed as *In the Matter of the Search of 2051 S. 102nd Street, Apartment E, West Allis*, No. 13-M-421.

allowing the FBI to enter and search Feldman's residence, including electronic storage media, for evidence of child pornography. (Aff. ¶¶ 9, 12.) The warrant was executed two days later. (Aff. ¶ 10.)

During the search, Banner spoke briefly to Feldman before he invoked his right to counsel. (Aff. ¶ 11.) Specifically, Feldman stated that he had lived at his current residence for the past 15 years, and that he was the sole occupant of the residence. (Aff. ¶ 30a.) Other evidence showed that Feldman is the only person paying taxes and receiving mail at his residence. (Aff. ¶ 30b-30c.) Feldman has a computer science degree from the University of Wisconsin–Madison. (Aff. ¶ 31c.) He is a longtime employee of Rockwell Automation, currently holding the title of Senior Software Development Engineer. (Aff. ¶ 31a.) In 2010, Feldman filed as a co-inventor for a U.S. patent for a "system and method for interfacing with an enterprise resource planning system." (Aff. ¶ 31b.)

Agents seized 16 storage devices during the search. (Aff. ¶ 12.) Five devices showed no traces of electronic data, and two devices were not encrypted. (Aff. ¶¶ 13-14.) The remaining nine devices contained data inaccessible due to encryption. (Aff. ¶¶ 15, 23.) The encryption programs on the storage devices appeared to be the sort that would lock or damage data if too many incorrect password guesses were made. (Aff. ¶¶ 17, 21a.) FBI analysts have spent over four months attempting to access the encrypted files without success. (Aff. ¶ 20.)

On one of the unencrypted devices, a Dell computer, FBI examiners found a peer-to-peer software program called "eMule." (Aff. ¶ 25.) Within eMule, log files indicated that 1,009 files were received, distributed, or stored using eMule, with most of the files having titles mainly indicative of child pornography.[3] (Aff. ¶ 25.) Examiners also found evidence that some of these files had been

[3] For example, two of the files were named "Pthc - !!!New Fucking 7 Yo Little Girl Hard Weekend3.mpg" and "Yoboy-Man-10Yo-Blonde-Boy-Sucks-And-Is-Anal-Fucked-15m35S.avi." (Aff. ¶¶ 25a, 25e.) "Pthc" is an abbreviation for "pre-teen hard core." (Aff. ¶ 27a.)

downloaded to various devices connected to the Dell computer—particularly, the "F," "G," and "I" drives. (Aff. ¶ 26.) The "I" drive corresponded to one of two encrypted devices. (Aff. ¶ 28a.) The "F" and "G" drives might correspond to any of the other connected devices. (Aff. ¶ 28b.) The Dell computer's login screen showed only one username, "Jeff." (Aff. ¶ 30d.)

II. DISCUSSION

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The Supreme Court has clarified that the Fifth Amendment "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); *see also United States v. Hubbell*, 530 U.S. 27, 34 (2000) ("The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character."). "[T]o be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210 (1988). Accordingly, the Court has declined to extend Fifth Amendment protection to, for example, the giving of blood samples and handwriting exemplars. *Fisher*, 425 U.S. at 408 (citing *Schmerber v. California*, 384 U.S. 757, 763-64 (1966), and *Gilbert v. California*, 388 U.S. 263, 265-67 (1967)).

"The act of *producing* evidence in response to a subpoena . . . has communicative aspects of its own, wholly aside from the *contents* of the papers produced." *Id.* at 410 (emphasis added); *see also Hubbell*, 530 U.S. at 36. This is because compliance with a subpoena tacitly concedes: (1) the existence of the documents, (2) their possession or control by the accused, and (3) the accused's belief that the documents are authentic. *Hubbell*, 530 U.S. at 36; *Fisher*, 425 U.S. at 410.

While compulsion is clearly present, the act of production nevertheless does not involve "testimonial" self-incrimination if "[t]he existence and location of the papers are a *foregone conclusion* and the [accused] adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." *Fisher*, 425 U.S. at 410-11 (emphasis added). Put differently, the contents of the accused's mind are not used against him where "the Government is in no way relying on the 'truth-telling' of the [accused] to prove the existence of or his access to the documents." *Id.* at 411. Thus, the issue is whether the production itself tells the government something it does not already know, which will "depend on the facts and circumstances of particular cases or classes thereof." *Id.* at 410.

In *Fisher*, the Supreme Court concluded that "compliance with a summons directing the [accused] to produce the accountant's documents . . . would involve no incriminating testimony within the protection of the Fifth Amendment." *Id.* at 414.[4] In *Hubbell*, the Court reached the opposite conclusion, holding that the accused's production in response to a subpoena calling for 11 broad categories of documents had "a testimonial aspect." 530 U.S. at 45. Critically, the Court in *Hubbell* distinguished *Fisher* because there, "the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them," whereas in *Hubbell*, "the Government ha[d] not shown that it had any

[4] In *Fisher*, each accused actually transferred possession of the documents in question to his attorney. *Id.* at 405. But because "the papers, if unobtainable by summons from the client, are unobtainable by summons directed to the attorney by reason of the attorney-client privilege," the Court proceeded to the question of whether the documents could have been obtained by summons from the accused while they were in his possession. *Id.*

prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by [the accused]." *Id.* at 44-45.

Since *Fisher*, at least four circuits have held that the government must establish its knowledge of the existence, possession, and authenticity of the subpoenaed documents with "reasonable particularity" before the "foregone conclusion" doctrine applies. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1344 & n.20 (11th Cir. 2012) (hereinafter, "*Subpoena Dated March 25, 2011*"); *United States v. Ponds*, 454 F.3d 313, 320-21 (D.C. Cir. 2006); *In re Grand Jury Subpoena, Dated April 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004); *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992*, 1 F.3d 87, 93 (2d Cir. 1993). Those courts have also cautioned, however, that "the 'reasonable particularity' standard cannot demand that the subpoena name every scrap of paper that is produced." *Ponds*, 454 F.3d at 325; *see also Subpoena Dated March 25, 2011*, 670 F.3d at 1347 (stating that the government need not "identify exactly the documents it seeks").

In 2012, the Eleventh Circuit became the first to weigh in on the precise issue involved here—namely, whether Fifth Amendment protection is available to an accused ordered to produce the decrypted contents of a computer.[5] In *Subpoena Dated March 25, 2011*, several pieces of the accused's digital media were seized pursuant to a search warrant during a child pornography investigation, but examiners were unable to access certain portions due to encryption. 670 F.3d at 1339. The government knew little about the encrypted portions; in fact, it conceded that, although encrypted, it was possible that the hard drives contained nothing. *Id.* at 1340. The accused objected to a grand jury subpoena, asserting that, "by decrypting the contents, he would be testifying that he, as opposed to some other

[5] As indicated by its case name, *Subpoena Dated March 25, 2011* involved a grand jury subpoena, whereas here, the court has been presented with an application under the All Writs Act. The difference, however, is immaterial to the Fifth Amendment analysis.

person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished." *Id.* at 1339-40.

After reviewing *Fisher* and *Hubbell*, the Eleventh Circuit analyzed whether the accused's decryption would sufficiently infringe on his Fifth Amendment privilege. *Id.* at 1346. First, the court rejected the government's contention that, because it only sought a physical act (that is, decryption), the accused's production would be a nontestimonial transfer, akin to providing a handwriting sample or standing in a lineup. *Id.* at 1345-46 & n.24. The court reasoned that, in both *Fisher* and *Hubbell*, the government merely sought a physical act (that is, the production of documents), but that fact was not dispositive. *Id.* at 1346. Therefore, the court concluded that both the production of documents and decryption "[are] accompanied by the implied factual statements noted above that could prove to be incriminatory," which makes those physical acts "testimonial in character." *Id.*

Nevertheless, because "an act of production is not testimonial—even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed materials—if the Government can show with 'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials," the Eleventh Circuit turned to the question of whether the "foregone conclusion" doctrine applied. *Id.* at 1346. The court found the doctrine inapplicable to its facts, reasoning as follows:

> Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that [the accused] is even capable of accessing the encrypted portions of the drives.

Id. at 1346. The court also noted that "there was no evidence that [the accused] was the only person who had access to his hard drives." *Id.* at 1340 n.9. Accordingly, the court found that the facts of its case were "far closer to the *Hubbell* end of the spectrum than . . . to the *Fisher* end." *Id.* at 1347.

The Eleventh Circuit also distinguished its facts from those in *In re Grand Jury Subpoena to Sebastien Boucher*, No. 06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009), where the accused accessed an encrypted portion of his computer in which a government agent had seen a file labeled "2yo getting raped during diaper change," and *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012), where the accused admitted that the content at issue was on her password-protected computer. *Subpoena Dated March 25, 2011*, 670 F.3d at 1348-49 & n.27. The court also suggested that "[k]nowledge of a file name, like the Government had in *Boucher*, would be 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.* at 1349 n.28.

Turning to the government's application here, although the issue is one of first impression, I am satisfied that the Seventh Circuit would adopt the test employed by its sister circuits in analyzing whether the "foregone conclusion" doctrine applies.[6] Accordingly, the question before the court is whether the government has established its knowledge of the existence, possession, and authenticity of the files on the encrypted storage devices with "reasonable particularity" such that Feldman's decryption would "add[] little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411.

[6] I am also satisfied that the Seventh Circuit would agree with the Eleventh Circuit that the fact that the government is only seeking to compel a physical act does not necessarily render the production a nontestimonial transfer.

Unlike in *Subpoena Dated March 25, 2011*, here, the government has shown that the encrypted devices contain data. In addition, during the search of the unencrypted Dell computer, the government found a peer-to-peer software program whose log files indicated that 1,009 files were received, distributed, or stored using the program, with most of the files having titles mainly indicative of child pornography. Examiners also found evidence that some of these files had been downloaded to various devices connected to the Dell computer, including one of two encrypted devices. In short, the government already knows the names of the files (which indicate child pornography) and their probable existence on the encrypted hard drives. Under these facts, "[t]he existence and location of the [files] are a foregone conclusion." *Id.*

Still, however, there is an issue of possession and authenticity. Feldman has a computer science degree, is a longtime employee of Rockwell Automation (currently, he holds the title of Senior Software Development Engineer), and filed as a co-inventor for a U.S. patent for a "system and method for interfacing with an enterprise resource planning system." Accordingly, unlike in *Subpoena Dated March 25, 2011*, here, the government has shown that Feldman may very well be *capable* of accessing the encrypted portions of the hard drives.

But the following question remains: Is it reasonably clear, in the absence of compelled decryption,[7] that Feldman actually *has* access to and control over the encrypted storage devices and, therefore, the files contained therein? To be sure, the storage devices were all found in Feldman's residence, where he has admittedly lived alone for the past 15 years. In addition, the unencrypted Dell computer, which showed connections to the encrypted storage devices, has a login screen with only one

[7] In the court's original order, filed on April 18, 2013, I mistakenly wrote "encryption," as opposed to "decryption" at this point in the text.

username, "Jeff." Nevertheless, unlike in *Boucher* and *Fricosu*, here, Feldman has not admitted access and control.

As the court stated in *Subpoena Dated March 25, 2011*,

> an act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic. The touchstone of whether an act of production is testimonial is whether the government compels the individual to use "the contents of his own mind" to explicitly or implicitly communicate some statement of fact.

670 F.3d at 1345 (internal citations omitted). This is a close call, but I conclude that Feldman's act of production, which would necessarily require his using a password of some type to decrypt the storage device, would be tantamount to telling the government something it does not already know with "reasonably particularity"—namely, that Feldman *has personal access to and control over* the encrypted storage devices. Accordingly, in my opinion, Fifth Amendment protection is available to Feldman. Stated another way, ordering Feldman to decrypt the storage devices would be in violation of his Fifth Amendment right against compelled self-incrimination.

NOW THEREFORE IT IS ORDERED that the government's "Application Under the All Writs Act Requiring Jeffrey Feldman to Assist in the Execution of Previously-Issued Search Warrant" be and hereby is **DENIED**.

SO ORDERED this 19th day of April 2013, at Milwaukee, Wisconsin

BY THE COURT:

s/ William E. Callahan, Jr.
WILLIAM E. CALLAHAN, JR.
United States Magistrate Judge