

8

Law Offices of Perry de Marco, Jr.  
BY: PERRY de MARCO, SR.  
Identification No. 90586  
Centre Square, West Tower  
1500 Market Street, Suite 4100  
Philadelphia, PA 19102  
215.563.6100

FILED

Attorney for Petitioner

AUG 27 2015

MICHAEL E. KUNZ, Clerk  
By \_\_\_\_\_ Dep. Clerk

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH  
OF SEIZED ITEMS:

- : Apple Mac Pro Computer
- : Apple iPhone 6 Plus Cellular Telephone
- : Western Digital My Book for Mac External
- : Hard Drive
- : Western Digital My Book VelociRaptor
- : Duo External Hard Drive
- : No. 15-850-M

MOTION TO QUASH GOVERNMENT'S APPLICATION TO COMPEL

It is respectfully suggested that the Honorable Court quash the government's application to compel respondent to divulge alleged passwords in his possession because said compulsion clearly violates his constitutional right against self-incrimination. The Self-Incrimination Clause of the Fifth Amendment of the United States Constitution states that "no person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. Nevertheless, "the privilege protects a person only against being incriminated by his own compelled testimonial communications." Fisher v. United States, 425 U.S. 391, 409 (1976), and where the communication is not testimonial, it is not protected by the Fifth Amendment. For example, documents voluntarily prepared by the defendant are not testimonial. Id. Thus, the privilege applies when the information being sought is compelled, incriminating in nature, and testimonial. Fisher, 425 U.S. at 408.

Respondent submits that the compelled production of the alleged passwords violates his Fifth Amendment privilege against self-incrimination. His act of production of the alleged passwords sought would be essentially testimonial as it would establish

the existence of certain proscribed materials, respondent's control over them, clearly potentially incriminating admissions. In order to overcome respondent's Fifth Amendment privilege, the Government must show with reasonable particularity that producing the records would convey no new information to the Government because the documents' existence, their control by respondent, and their authenticity were a "foregone conclusion" at the time the Summons was issued in 2013. Here, the Government has not discharged its heavy burden of establishing these facts, or, indeed, any one of these three requirements and the application should be quashed.

#### THE ACT OF PRODUCTION PRIVILEGE

It is beyond cavil that respondent has an absolute privilege under the Fifth Amendment to refuse to produce the passwords sought by the government. Any response to the summons would manifest and establish the existence and his possession or control of the electronic devices at issue, as well as implicitly authenticate them. United States v. Hubbell, 530 U.S. 27, 36-37 (2000); United States v. Fox, 721 F.2d 32, 36-39 (2d Cir. 1983). Divulging the passwords could provide, at a minimum a potential link in a chain of incriminating evidence. Hoffman v. United States 341 U.S. 479, 486, (1951) (holding that the Fifth Amendment covers evidence "which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime").

The leading case on the act of production doctrine now is United States v. Hubbell, 530 U.S. 27 (2000), wherein the Supreme Court held that, unless the Government has specific knowledge of the existence of particular documents in an individual's possession, it cannot compel production of documents, even business records, from an individual in the face of a valid assertion of the individual's Fifth Amendment privilege. 530 U.S. at 44-45, 120 S. Ct. at 2048. The Court stated that when an individual is compelled to identify and produce documents which the Government was previously unaware he possessed or that existed, the act of producing the documents is "tantamount to answering a series of interrogatories

asking a witness to disclose the existence and location of particular documents." Id., 530 U.S. at 31. Following the production of documents under compulsion the use of the documents or their contents, which otherwise are not privileged, violates the Fifth Amendment. Id., 530 U.S. at 42-43. Accordingly, it is submitted that compelling respondent to divulge the requested passwords constitutes an act covered by the Fifth Amendment and the government has a burden to show why respondent's constitutional right not to incriminate himself would not be infringed.

#### THE FOREGONE CONCLUSION DOCTRINE

Instantly, the government recognizes that respondent is being compelled to divulge the passwords and that doing so would be incriminating under the Fifth Amendment right but states that requiring respondent to divulge the passwords is not testimonial because it is purportedly aware of what is contained on the electronic devices at issue, *i.e.*, that their contents are a "foregone conclusion" and respondent cannot stand behind the Fifth Amendment and refuse to divulge the passwords it requests. However, unless the Government demonstrates a "foregone conclusion" as to the existence, location and authenticity of records, such that "the question is not of testimony but of surrender," Fisher, 425 U.S. at 411, the act of producing the passwords warrants constitutional protection. Here, the government below asserts that the testimonial aspects of the act of production are a "foregone conclusion" because of viewed image labels and images certain family members viewed and thus, the act of production would convey no information that it did not already have.

However, in order to defeat respondent's Fifth Amendment privilege claim under the "foregone conclusion" doctrine, the Government must "establish its knowledge of the existence, possession and authenticity of subpoenaed documents with 'reasonable particularity'." United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999) (emphasis added), *aff'd*, 530 U.S. 27, 120 S.Ct. 2032 (2000). The burdens of proof and production as to a "foregone conclusion" are on the Government. In re Grand Jury Subpoena dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004); In re Grand Jury Proceedings, 41 F.3d 377, 380 (8th Cir. 1994). The Government must

show that it had the requisite knowledge at the time it issued the Summons. Grand Jury Subpoena dated April 18, 383 F.3d at 911; Hubbell, 167 F.3d at 569. This is a high burden as the Government must demonstrate "that the United States knows, as a certainty, that each of the myriad of documents demanded" is possessed or controlled by defendant. United States v. Doe, 465 U.S. 605, 613 fn.12, (1984 ). The government must also offer "evidence" establishing that the documents can be "independently authenticated." In re Grand Jury Proceedings, 41 F.3d at 388. Finally, the government's knowledge must be sufficient to "eliminate any possibility that the witness' production would constitute an incriminating testimonial act." United States v. Fox, 721 F.2d 32, 37-38 (C.A.N.Y. 1983).

The foregone conclusion analysis is highly dependent on "the facts and circumstances of particular cases." Fisher, 425 U.S. at 410. In evaluating claims of "foregone conclusion," courts are careful to differentiate between requests for documents whose specific existence or location had been proven or admitted and more general requests for categories of documents whose existence is merely presumed. For example, in Grand Jury Subpoena dated April 18, supra, the Government sought a wide variety of records from a witness it had interviewed regarding an antitrust investigation relating to sales of computer memory chips. In the interview, the witness said he had sent specific emails relating to his conversations about pricing information, but that he had no other records. Id. at 908. At the close of the interview, the Government served a broad subpoena seeking inter alia calendars, notepads, or "any similar documents" relating to sales or production of the products at issue. Id. The Ninth Circuit quashed the subpoena and reversed the district court's finding of contempt, holding that the Government had failed to demonstrate the existence of and possession of the records with "reasonable particularity" since the only records it knew about were the few emails the witness had described. Id. at 910-11. While the existence and location of the emails the witness had admitted he sent were a "foregone conclusion," the court rejected a further claim that because the witness was a salesman he could be assumed to "always possess business records describing or memorializing meetings or prices"; such an assumption "does not establish the reasonably particular knowledge required." Id. at 911-12; see also United

States v. Bright, 596 F.3d 683, 692-93 (9th Cir. 2010) (upholding finding of "foregone conclusion" for specific records previously known to the Government but reversing for generalized request for other records).

Instantly, respondent submits that simply because certain relatives may have allegedly observed certain images on respondent's devices and advised government agents of them, does not establish that they currently are contained in files saved on the devices. No where set forth in the government's presentation is an indication that it can advert with the required degree of certainty that there is child pornography stored on the devices. At this moment, the allegations remain just that, allegations, which as noted above are insufficient to apply the foregone conclusion doctrine.

Respondent relies on In re Grand Jury Subpoena Duces Tecur (Doe), 670 F.3d 1335 (11th Cir. 2012), wherein FBI agents seized several laptop computers and external hard drives the FBI believed contained child pornography that could not be accessed because the data was encrypted. The question before the Court was whether compelling Doe to reveal the decrypted data violated the right against self-incrimination. The Doe Court ruled that because the government did not have specific enough knowledge of what the devices may contain, the foregone conclusion doctrine did not apply and Doe did not have to assist the agents in decrypting what, if, anything, may have been saved in the devices.

Respondent submits that Doe controls here and thus, that the process filed by the government should be quashed. Thus, because the location, existence, and authenticity of the purported evidence is not known to the government, the Fifth Amendment applies because the government demands that respondent use the contents of his mind against himself, Fifth Amendment protection is available. It is the compelling an accused to provide a password or decrypt a device for the government to gain access to information violates the Fifth Amendment privilege reflects consistent Supreme Court precedent. See, *i.e.*, Couch v. United States, 409 U.S. 322, 328 (1973) ("it is extortion of information from the accused \*16 himself that offends our sense of justice.") and United States v. Hubbell, 530 U.S. at 37 ("whether the constitutional privilege protects... the act of production itself, is a question that is

distinct from the question whether the unprotected contents of the documents themselves are incriminating.").

In conclusion, it is respectfully requested that the Honorable Court rule that respondent has a valid Fifth Amendment claim not to divulge any passwords and the government's process be quashed because the government has not established with the requisite degree of certainty that it is aware of the contents of the devices

Respectfully Submitted,

  
FERRY de MARCO, JR.  
Attorney for Petitioner