

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge Robert E. Blackburn**

Criminal Case No. 10-cr-00509-REB-02

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. RAMONA CAMELIA FRICOSU,
a/k/a Ramona Smith,

Defendant.

**ORDER GRANTING APPLICATION UNDER THE ALL WRITS
ACT REQUIRING DEFENDANT FRICOSU TO ASSIST IN THE
EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS**

Blackburn, J.

The matters before me are (1) the government's **Application Under the All Writs Act Requiring Defendant Fricosu To Assist in the Execution of Previously Issued Search Warrants** [#111]¹ filed May 6, 2011; and (2) **Ms. Fricosu's Motion for Discovery – Seized Hard Drive** [#101] filed April 27, 2011. I held hearings on these motions on November 1, 2011, and January 3, 2012, at which I received evidence and argument.

In fashioning my ruling, I have considered all relevant adjudicative facts in the file and record of this case. I have considered the evidence educed at the hearings on November 1, 2011, and January 3, 2012. I have considered, but not necessarily

¹ “[#111]” is an example of the convention I use to identify the docket number assigned to a specific paper by the court's electronic case filing and management system (CM/ECF). I use this convention throughout this order.

accepted, the reasons stated, arguments advanced, and authorities cited by counsel in their papers and during oral argument at the conclusion of the hearing on January 3, 2012.

In assessing the credibility of the witnesses who testified during the hearings, I have considered all facts and circumstances shown by the evidence that affected the credibility of each witness, including the following factors: the witness's means of knowledge, ability to observe, and strength of memory; the manner in which he or she might be affected by the outcome of the hearing; the relationship he or she has to either side in the case; and the extent to which, if at all, he or she was either supported or contradicted by other evidence presented during the hearing.

I have considered the totality of relevant circumstances. My findings of fact are based on a preponderance of the evidence. Any finding of fact more properly deemed a conclusion of law, or any conclusion of law more properly deemed a finding of fact, shall be as more properly characterized.

I. FINDINGS OF FACT

On May 14, 2010, the FBI executed a search warrant at 10436 Ross Lake Drive in Peyton, Colorado, where defendant, Ramona Fricosu lived with her children and her mother. At the time of the search, Ms. Fricosu and her husband, co-defendant Scott Whatcott, were divorced, and Mr. Whatcott was incarcerated at the Four Mile Correctional Center in Pueblo, Colorado, on state charges.

During the search, agents seized, *inter alia*, six computers. Agents seized three desktop computers, which are not implicated by the present motion. The remaining three computers were laptops, more specifically: (1) a Hewlett-Packard 6001; (2) a

Toshiba 7600; and (3) a Toshiba Satellite M305. Neither the Hewlett-Packard nor the Toshiba 7600 was encrypted, and investigative agents were able to image and examine their contents.² The Toshiba Satellite M305, however, was password-protected by a program called PGP Desktop, and agents have been unable to decrypt it.

The Toshiba Satellite M305 laptop computer was found in Ms. Fricosu's bedroom during the search. When agents started the computer, they were able to view the whole disk encryption screen,³ which identifies the computer as "RS.WORKGROUP.Ramona." (Gov't Hrg. Exh. 2B at 2.) FBI Special Agent Travis Johnson testified at the hearing that "WORKGROUP" is the default network designation that the computer assigns if the user does not choose another name for his or her network during the initial set up of the computer. The final designation also is made during the initial set up and indicates the account name.⁴

The day following the execution of the search warrant, Mr. Whatcott called Ms. Fricosu from the Four Mile Correctional Center. Their conversation was recorded. During that call, the following relevant exchange occurred:

Ramona: Oh so anyway, earlier we were talking about that lawyer thing
Scott: Yes
Ramona: So um, in a way I want them to find it

² Investigation of the Hewlett-Packard laptop revealed documents that the examining agent believed might be potentially privileged communications between Mr. Whatcott and his attorney; thus, further examination of that computer was halted. The Toshiba 7600 was examined and determined to belong to Ms. Fricosu's mother, Elena Visardi, and has since been returned to her.

³ The computer screen was damaged such that the use of an external monitor was necessary to view the contents of the screen.

⁴ The registry keys of the other two laptop computers identified the "Registered Owner" of the Hewlett Packard laptop as "Scott" and of the Toshiba 7600 as "Elena."

Scott: OK

Ramona: in a way I don't just for the hell of it

Scott: OK

....

Ramona: Ookay (pause) uhm in a way I want them to find it

Scott: Mm-hmm

Ramona: and uhm because they will have to ask for my help uhm and in another way I don't want them to find it let them let them work for it

Scott: Right

Ramona: you know what I mean

Scott: right (pause) yeah, if it's there, they, they will find it

Ramona: uhm, can they get past what they need to get past to get to it

Scott: they will listen first

Ramona: it will shut off

Scott: (pause) what

Ramona: it was on my laptop

Scott: oh yeah

Ramona: yeah

Scott: OK

Ramona: I don't know if they can get to it

Scott: it was on your laptop

Ramona: yes

Scott: OK (pause) and did you have any something like anything on your computer to protect it or something

Ramona: yeah

Scott: OK then I don't know.

Ramona: I mean, I think I did

Scott: OK

Ramona: Ya know I haven't

Scott: (SC [simultaneous conversation]) oh yeah that's right it was on your laptop wasn't it

Ramona: I think so but I'm not sure

Scott: OK

Ramona: yeah cause they kept asking me for passwords and I said, ya know no I just didn't answer them

Scott: right (SC). Because when you went there you took your laptop

Ramona: yeah I think so I think I did

Scott: and so (SC) it would been on there

Ramona: yeah

Scott: OK

Ramona: and my lawyer said I'm not obligated by law to give them any passwords or anything they need to figure things out for

themselves

(*Id.*, Gov't Hrg. Exh. 8 at 1-3.) Based on this conversation, the government sought a warrant to allow it to search the Toshiba Satellite M305 laptop. By this motion, the government seeks a writ pursuant to the All Writs Act, 28 U.S.C. § 1651, requiring Ms. Fricosu to produce the unencrypted contents of the computer. She has declined, asserting her privilege against self-incrimination under the Fifth Amendment.

Based on a preponderance of the evidence, I find that the Toshiba Satellite M305 laptop computer belongs to Ms. Fricosu, or, in the alternative, that she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer.

II. CONCLUSIONS OF LAW

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. Nevertheless, “the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence.” *Fisher v. United States*, 425 U.S. 391, 408, 96 S.Ct. 1569, 1579, 48 L.Ed.2d 39 (1976). Instead, “the privilege protects a person only against being incriminated by his own compelled testimonial communications.” *Id.*, 96 S.Ct. at 1580.

Although the privilege applies typically to verbal or written communications, an act that implicitly communicates a statement of fact may be within the purview of the privilege as well. *United States v. Hubbell*, 530 U.S. 27, 36, 120 S.Ct. 2037, 2043, 147 L.Ed.2d 24 (2000); *Doe v. United States*, 487 U.S. 201, 209, 108 S.Ct. 2341,

2347, 101 L.Ed.2d 184 (1988) (*Doe II*). More specifically in the context of this case, “[a]lthough the contents of a document may not be privileged, the act of producing the document may be.” *United States v. Doe*, 465 U.S. 605, 612, 104 S.Ct. 1242, 1242, 79 L.Ed.2d 552 (1984) (*Doe I*).⁵ Production itself acknowledges that the document exists, that it is in the possession or control of the producer, and that it is authentic. *Hubbell*, 120 S.Ct. at 2043.

The small universe of decisions dealing with the Fifth Amendment issues implicated by compelling a witness or defendant to provide a password to an encrypted computer or otherwise permit access to its unencrypted contents are instructive here. In *In re Grand Jury Subpoena to Boucher*, 2007 WL 4246473 (D. Vt. Nov. 29, 2007) (*Boucher I*), a laptop computer was found in the defendant’s car during a search incident to his crossing the border from Canada into the United States. During the initial search, an officer opened the computer and without entering a password was able to view its files, revealing thousands of images of what appeared to be, based on the names of the files, adult and some child pornography. An agent of the Bureau of Immigration and Customs Enforcement (“ICE”) was called in, who asked the defendant to show him where these images were located on the computer.⁶ The defendant navigated to a drive “Z,” which contained several images of child pornography. After the

⁵ The contents of the computer are not, and are not claimed to be, privileged. *See Doe I*, 104 S.Ct. at 1241-42 (documents that are prepared or compiled voluntarily lack the element of compulsion and are not protected by the Fifth Amendment); *In re Grand Jury Subpoena to Boucher*, 2009 WL 424718 at *2 (D. Vt. Feb. 19, 2009) (same, with respect particularly to contents of a laptop computer).

⁶ The defendant had acknowledged that he sometimes downloaded child pornography unknowingly from online newsgroups, but stated that he deleted all such files when he realized their contents.

defendant was arrested and the laptop seized, the computer was found to be password-protected. When agents were unable to decrypt the computer, the grand jury issued a subpoena demanding the defendant produce any documents reflecting any passwords associated with the computer. **Boucher I**, 2007 WL 4246473 at *1-2. Noting that under prevailing Supreme Court precedent, a defendant cannot be compelled to reveal the contents of his mind, the magistrate judge found that the act of producing the password was testimonial and, therefore, privileged. *Id.* at *4-*6. **Accord United States v. Kirschner**, 2010 WL 1257355 at *3-4 (E.D. Mich. March 30, 2010).

On appeal of that decision, the grand jury revised its request to require the defendant to produce, not the password itself, but rather an unencrypted version of the Z drive. **In re Grand Jury Subpoena to Boucher**, 2009 WL 424718 at *2 (D. Vt. Feb. 19, 2009) (**Boucher II**). Because of the revision to the request, the district court denied the motion to quash. The court noted that “[w]here the existence and location of the documents are known to the government, no constitutional rights are touched, because these matters are a foregone conclusion,” that is, they “add[] little or nothing to the sum total of the Government’s information.” *Id.* at *3 & *4 (quoting **Fisher**, 96 S.Ct. at 1581) (internal quotation marks omitted). Likewise, the defendant’s production was not necessary to authenticate the drive because he had already admitted possession of the computer, and the government had agreed not to use his act of production as evidence of authentication. *Id.* at *4. **Accord United States v. Gavegnano**, 2009 WL 106370 at *1 (4th Cir. Jan. 16, 2009) (where government independently proved that defendant was sole user and possessor of computer, defendant’s revelation of password not subject to

suppression).

There is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production. *See Boucher II*, 2009 WL 424718 at *3 (citing *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992*) (*United States v. Doe*), 1 F.3d 87, 93 (2nd Cir. 1993), *cert. denied*, 114 S.Ct. 920 (1994)).

Additionally, I find and conclude that the government has met its burden to show by a preponderance of the evidence that the Toshiba Satellite M305 laptop computer belongs to Ms. Fricosu, or, in the alternative, that she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer. The uncontroverted evidence demonstrates that Ms. Fricosu acknowledged to Whatcott during their recorded phone conversation that she owned or had such a laptop computer, the contents of which were only accessible by entry of a password. Of the three laptop computers found and seized during the execution of the search warrant of Ms. Fricosu's residence, only one was encrypted, the Toshiba Satellite M305. That laptop computer was found in Ms. Fricosu's bedroom, and was identified as "RS.WORKGROUP.Ramona." None of defendant's countervailing arguments – the suggestions that the computer might have been moved during the search, that someone else may have randomly designated the computer account as "Ramona," or that the fact that the hard drive was imaged before it was read somehow undermines its validity or

authenticity⁷ – is sufficient to alter my conclusion that it is more likely than not that the computer belonged to and was used by Ms. Fricosu. Accordingly, I find and conclude that the Fifth Amendment is not implicated by requiring production of the unencrypted contents of the Toshiba Satellite M305 laptop computer.

It is clear that the All Writs Act enables the court to issue orders to effectuate an existing search warrant. **See *United States v. New York Telephone Co.***, 434 U.S. 159, 172, 98 S.Ct. 364, 372, 54 L.Ed.2d 376 (1977) (“This Court has repeatedly recognized the power of a federal court to issue such commands under the All Writs Act as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.”); **see also *In re Application of United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone***, – F.Supp.2d – , 2011 WL 3424470 at *44 (D. Md. Aug. 3, 2011) (citing cases in which All Writs Act used to effectuate existing search or arrest warrant). Moreover, the government has offered Ms. Fricosu immunity, precluding it from using her act of producing the unencrypted contents of the laptop computer against her. (**See** Gov’t Motion App., Exh. 1.) Accordingly, the writ should issue.

THEREFORE, IT IS ORDERED as follows:

1. That the government’s **Application Under the All Writs Act Requiring Defendant Fricosu To Assist in the Execution of Previously Issued Search**

⁷ Special Agent Johnson testified in detail as to the verification procedures he used to ensure that the imaged copy was what it purported to be. Proof at the level of abstraction that Ms. Fricosu suggested was necessary at the hearing is not necessary and probably ultimately not available in any event.

Warrants [#111] filed May 6, 2011, is **GRANTED**;

2. That **Ms. Fricosu's Motion for Discovery – Seized Hard Drive** [#101], filed April 27, 2011, is **GRANTED**;

3. That on or before **February 6, 2012**, the government **SHALL PROVIDE** counsel for defendant, Ramona Camelia Fricosu, with a copy of the hard drive of the Toshiba Satellite M305 laptop computer, serial number 98158161W;

4. That on or before **February 21, 2012**, defendant, Ramona Camelia Fricosu, **SHALL PROVIDE** counsel for the government in this case with an unencrypted copy of the hard drive of the Toshiba Satellite M305 laptop computer, serial number 98158161W; and

5. That the government **SHALL BE** precluded from using Ms. Fricosu's act of production of the unencrypted contents of the computer's hard drive against her in any prosecution.

Dated January 23, 2012, at Denver, Colorado.

BY THE COURT:



Robert E. Blackburn
United States District Judge