IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 10-cr-00509-01-REB

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. RAMONA CAMELIA FRICOSU,
aka Ramona Smith,

Defendant.

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

I. INTRODUCTION

The United States of America, by and through John F. Walsh, United States Attorney, and Patricia Davies, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring the defendant Ramona Friscosu, to assist in the execution of federal search warrants by making available the unencrypted contents of a Toshiba Laptop – Satellite M305 ("Subject Computer"), previously seized and authorized for search under warrants in 10-sw-5230-MJW and 10-sw-05377-MJW.

II. BACKGROUND

The Federal Bureau of Investigation ("FBI") currently has in its possession the Subject Computer, which was seized pursuant to a search warrant issued by this Court, in 10-sw-5230-MJW. Investigative agents also sought and obtained a further warrant to search the Subject Computer for additional items in 10-sw-05377-MJW. Initial inspection of the Subject Computer revealed that it is encrypted. Because it is encrypted, law enforcement agents are not able to examine the Subject Computer as commanded by the search warrants in 10-sw-5230-MJW and 10-sw-05377-MJW.

The Subject Computer is a Toshiba Laptop – Satellite M305, Serial # 98158161W. The Subject Computer was seized from the residence inhabited by Ms. Fricosu, her two minor children, and Ms. Fricosu's mother. At the time of seizure, the Subject Computer was resting on top of its laptop case in Ms. Fricosu's bedroom. To resolve a discovery dispute, the government's counsel previously requested of Ms. Fricosu's counsel that she provide the password to the Subject Computer. Ms. Fricosu's counsel responded, in substance, that Ms. Fricosu has no obligation to assist law enforcement, and thereafter, filed a motion seeking a copy of the encrypted drive. (Document # 101).

This Application seeks an order requiring Ms. Fricosu to make available the unencrypted contents of the Subject Computer. This could be accomplished by having the encrypted Subject Computer available in the courtroom. Upon order of the court, Ms. Fricosu could enter the password without being observed by the government, or

otherwise provide the unencrypted contents of the Subject Computer by means she chose.[1] The requested order would thus allow the agents to comply with the two prior search warrants issued by this Court.

III. DISCUSSION

A. This Court May Properly Order The Requested Relief Pursuant to the All Writs Act

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Service,* 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice." *United States v. New York Tel. Co.,* 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.,* the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing

---

[1]. If the requested relief is granted, the government would arrange to have computer forensic personnel standing by to prepare a forensic image of the unencrypted version immediately. The unencrypted version could be further copied for each of the defendants.

a pen register. Consequently, this Court has the authority to order Ms. Fricosu to make available an unencrypted version of the Subject Computer to effectuate the previously issued search warrants in 10-sw-5230-MJW and 10-sw-05377-MJW.

The government obtained the Subject Computer in conformity with the Fourth Amendment; that is, by application to this court for search warrants based upon a probable cause showing. This court issued two search warrants, referenced above, for the Subject Computer. This court should now issue the order requested because doing so would enable agents to comply with this court's warrants commanding that the Subject Computer be examined for evidence identified by the warrants. Examining the Subject Computer further in its current state to attempt access to its unencrypted contents, if it is possible at all, would require significant resources and may harm the Subject Computer.

B. Any Fifth Amendment Right of Defendant Is Properly Addressed by "Act of Production Immunity"

1. Facts Relevant to Fifth Amendment Analysis

As an initial matter, the following facts are worth noting:

First, the government knows that the encrypted drive exists on Ms. Fricosu's laptop computer because it was validly obtained by search warrant and is in the government's possession. The government also has sound bases to believe that the Subject Computer contains evidence relevant to the charged offenses. The charged offenses were facilitated substantially by computers. Moreover, "back up" electronic

part of evidence developed from information contained in the documents that the defendant produced. In affirming dismissal of the indictment, the Court held that the immunity granted in the prior prosecution in exchange for disclosure precluded subsequent unrelated prosecution because the testimonial aspect of defendant's act of production was a necessary first step in discovering evidence supporting the second prosecution. The Court described the broad subpoena as the equivalent of "a detailed written interrogatory or a series of oral questions at a discovery deposition." *Id.* at 41-42.

This case shares none of *Hubble*'s defining characteristics. The government knows that an unencrypted version of the drive exists on the defendant's laptop. The government knows that the Subject Computer has a very high likelihood of containing evidence pertaining to the charged crimes for the reasons noted above. The government knows that the defendant had access to, and control over, the Subject Computer immediately prior to the search warrant execution because it was found in her bedroom, on top of the laptop case.

3. The Government Requests That This Court Order Act of Production Immunity To Address Defendant's Limited Fifth Amendment Right

As the act of production might potentially entitle Ms. Fricosu to assert her right to refuse under the Fifth Amendment of the United States Constitution, the Government has sought approval to seek this court's grant of limited immunity, thus precluding the Government from using her act of producing the unencrypted contents against her in

any prosecution.[2] No other basis exists upon which Ms. Fricosu might legally assert the right to refuse to provide the unencrypted contents. (A proposed order will be submitted prior to any hearing on this Application).

Only when an "act of production" explicitly or implicitly communicates facts or information otherwise protected by the Fifth Amendment privilege against testimonial self-incrimination – for example, if the existence and location of subpoenaed records are unknown to the Government, or where the mere act of production would authenticate the records – does the act of production fall within the scope and protection of the defendant's Fifth Amendment privilege. *See Fisher*, 425 U.S. at 409-411 (holding that production of documents within possession of taxpayer's attorneys did not implicate the taxpayer's Fifth Amendment privilege; where the "existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers"); *Doe*, 487 U.S. at 210-215 (holding that the target of a fraud investigation could be compelled to sign consent to allow foreign banks to release his banking records, since signing of the consent form itself communicated no information to the Government).

---

[2]This Application is made with approval from Kenneth A. Blanco, Deputy Assistant Attorney General of the Criminal Division of the Department of Justice, pursuant to the authority vested in him by Title 18, United States Code, Section 6003(b), and Title 28, Code of Federal Regulations, Section 0.175(a). A copy of the document from the Deputy Assistant Attorney General expressing such approval is attached hereto as Exhibit A.

storage devices also obtained during the search contain documents relating to the charged wire fraud, bank fraud and false statement offenses.

Second, Ms. Fricosu's voluntary conduct has linked her to the contents of the encrypted drive. It was found on the floor of her bedroom sitting on top of its laptop case. And, as set forth in the application and affidavit in 10-sw-05377-MJW, Ms. Fricosu discussed the Subject Computer with co-defendant and ex-spouse Scott Whatcott while he was incarcerated (and the telephone call was being recorded) and referenced specific information relevant to the case that the Subject Computer contains.

Third, the government already possesses, in an encrypted format, Ms. Fricosu's drive. This is not a situation where the government seeks to compel a defendant to produce items that may potentially be incriminatory and her act of producing them arguably has evidentiary value to authenticate the items.

Fourth, the government only requires that Ms. Fricosu's produce the contents of the drive in an unencrypted format. The government does not request that Ms. Fricosu give the government access to the password to the drive, either orally or in written form.

Fifth, as discussed further below, it is undisputed that the contents of Ms. Fricosu's encrypted drive are not protected under the Fifth Amendment because the files were created voluntarily and prior to the execution of the search warrants in 10-sw-05230-MJW and 10-sw-05377-MJW.

2. Defendant's Fifth Amendment Right Vis-a-vis Producing The Unencrypted Contents is Limited

The Government needs access to the unencrypted contents of the digital media in order to effectuate this Court's prior search warrants. In essence, although the government has complied with the Fourth Amendment in obtaining the Subject Computer, defendant thwarts lawful investigation. It is beyond cavil that the contents of the encrypted drive were created and compiled voluntarily and therefore do not enjoy Fifth Amendment protection simply because they may prove incriminatory or may in some way add to the government's case. *See Baltimore City Dep't of Soc. Servs. v. Bouknight*, 493 U.S. 549, 555 (1990); *In re: Grand Jury Subpoena to Sebastian Boucher*, 2009 WL 424718 (D. Vt. February 19, 2009) (involving an encrypted computer), *citing Fisher v. United States*, 425 U.S. 391 (1976) and *Doe v. United States,* 487 U.S. 201 (1988). The court should ignore any suggestion that the contents of the Subject Computer are protected simply because they may be incriminatory.

In *United States v. Hubbell*, 530 U.S. 27 (2000), the Supreme Court gave guidance regarding the scope of Fifth Amendment protection. There, the government had no knowledge of the existence or whereabouts of subpoenaed documents. *Id.* at 45. In fact, when the grand jury issued the subpoena, the government was investigating a matter entirely different from the charges ultimately brought. *Id.* at 31-32. The subpoena itself required the production of 11 "broadly worded" categories of documents and the defendant ultimately produced 13,120 pages following the granting of immunity. *Id.* at 42. The government later attempted to prosecute for different crimes based in

The only Court that has specifically considered whether a target may be compelled to provide the unencrypted contents of a computer seized pursuant to a warrant ruled the target had no act of production privilege to refuse to provide the Grand Jury with an unencrypted version of the hard drive of his computer (by entering his password information), since "providing access to the unencrypted drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information." *Boucher, supra,* 2009 424718 WL at *3-4 (*quoting Fisher*, 425 U.S. at 411). *Cf. United States v. Kirschner*, 2010 WL 1257355 (E.D. Mich. March 30, 2010) (finding that a subpoena which required target to actually respond to questioning and provide verbal testimony regarding his password did implicate the target's Fifth Amendment privilege). The *Boucher* Court noted, however, that the Government could not make use of the target's act of production to authenticate the unencrypted drive or its contents; essentially holding that the subpoena implicitly conferred upon the target limited use immunity for the act of producing the unencrypted contents of the seized computer. *Boucher, supra,* 2009 424718 WL at *3-4 . Thus, requiring Ms. Fricosu to provide the Government with access, by entering the necessary encryption keys to the digital media that the Government already possesses pursuant to a valid search and seizure warrant, amounts to compelling Ms. Fricosu only "to surrender the key to a strongbox containing incriminating documents." *Fisher*, 425 U.S. at 408, n. 9.

Public interests will be harmed absent requiring defendants to make available unencrypted contents in circumstances like these. Failing to compel Ms. Fricosu

amounts to a concession to her and potential criminals (be it in child exploitation, national security, terrorism, financial crimes or drug trafficking cases) that encrypting all inculpatory digital evidence will serve to defeat the efforts of law enforcement officers to obtain such evidence through judicially authorized search warrants, and thus make their prosecution impossible.

WHEREFORE, the United States of America respectfully requests that the Court issue an Order granting the Application Under the All Writs Act to require Ms. Fricosu to produce the unencrypted contents of the Subject Computer, and granting her act of production immunity in connection therewith.

Dated this 6th day of May, 2011

JOHN F. WALSH
United States Attorney

By: s/Patricia Davies
PATRICIA DAVIES
Assistant United States Attorney
United States Attorney's Office
1225 17th Street, Suite 700
Denver, CO 80202
Phone: 303/454-0100
Fax: 303/454-0401
patricia.davies@usdoj.gov
Attorney for Government

CERTIFICATE OF SERVICE

I hereby certify that on this 6nd day of May, 2011, I electronically filed the foregoing **APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT FRICOSU TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS** with the clerk of the Court using the CM/ECF system which will send notification of such filing to the following email addresses:

Mark Johnson
mark.johnson68@gmail.com

Philip L. Dubois
dubois@dubois.com

Tonya Andrews
Tonya.Andrews@usdoj.gov

Martha Paluch
Martha.Paluch@usdoj.gov

By: s/ Maureen Carle

MAUREEN CARLE
Legal Assistant
1225 Seventeenth Street, Suite 700
Denver, Colorado 80202
Telephone: (303) 454-0100
Facsimile: (303) 454-0406
E-mail: Maureen.Carle@usdoj.gov

USA v. RAMONA FRICOSU
CASE #: 1:10-CR-00509-REB-02

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

EXHIBIT 01

U.S. Department of Justice

Criminal Division

Assistant Attorney General *Washington, D.C. 20530*

MAY - 5 2011

The Honorable John F. Walsh
United States Attorney for the
District of Colorado
1225 Seventeenth Street
Suite 700
Denver, Colorado 80202

Attention: Patricia Davies
Assistant United States Attorney

Re: *United States v. Ramona Fricosu*

Dear Mr. Walsh:

Pursuant to the authority vested in me by 18 U.S.C. § 6003(b) and 28 C.F.R. § 0.175(a), I hereby approve your request for authority to apply to the United States District Court for the District of Colorado for an order, pursuant to 18 U.S.C. §§ 6002-6003, requiring Ramona Camelia Fricosu to give testimony or provide other information in the above matter and in any further proceedings resulting therefrom or ancillary thereto, provided that the testimony or other information from such individual may be necessary to the public interest, and that such individual refuses to testify or provide information on the basis of the privilege against self-incrimination.

Sincerely,

Lanny A. Breuer
Assistant Attorney General

KENNETH A. BLANCO
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION