IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 10-cr-00509-REB-2

UNITED STATES OF AMERICA,

Plaintiff,

v.

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

Defendant.

GOVERNMENT'S REPLY TO AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT FRICOSU'S OPPOSITION TO GOVERNMENT'S APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS (Docket #172-1) and MS. FRICOSU'S RESPONSE TO DOCUMENT 111 (Docket #174)

The United States of America, by and through the undersigned Assistant United States Attorneys, replies to Amicus Curiae Brief of Electronic Frontier Foundation in Support of Defendant Fricosu's Opposition to Government's Application under the All Writs Act Requiring Defendant to Assist in the Execution of Previously Issued Search Warrants (Docket #172-1) and Ms. Fricosu's Response to Document 111 (Docket #174) as follows:

A. The All Writs Act authorizes this Court to issue orders upholding its search warrants

Ms. Fricosu challenges the appropriateness of using an All Writs Act order, 28 U.S.C. § 1651(a). However, the Supreme Court has explicitly endorsed the use of the All Writs Act to ensure that a court's search warrants are not frustrated. The Court held that the All Writs Act permits federal courts to "issue such commands… 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." *United States v. New York Tel. Co.,* 434 U.S. 159, 172 (1977). *New York Telephone* explicitly applied to a search warrant; the Court even explained how Rule 41 (the Federal Rule of Criminal Procedure governing the issuance of search warrants) applied. *Id.* at 168-70.

While Ms. Fricosu suggests that *New York Telephone Company* was the only case to apply the All Writs Act to search warrants, (Doc. 174 at 2), in fact the use of the All Writs Act in support of search warrants is well-established. In the years before Congress enacted the Pen Register and Trap and Trace Statute in 1986, *see* 18 U.S.C. §§ 3121 et seq., the government often used the All Writs Act in support of search warrants to compel telephone companies to assist in the "search" for dialed phone numbers. For example, in *Application of United States for an Order Authorizing an In-Progress Trace of Wire Communications over Tel. Facilities,* 616 F.2d 1122 (9th Cir. 1980), the Court held that "the Order of the district court was a proper exercise of its discretion under Rule 41 and the All Writs Act." *Id.* at 1132. *See also Application of United States for Order Authorizing Installation of Pen Register or Touch-Tone Decoder and Terminating Trap,* 610 F.2d 1148, 1155 (3d Cir. 1979) ("The telephone companies in the present cases fall within the reach of the district courts' All Writs Act powers…"); *Michigan Bell Tel. Co. v. United States,* 565 F.2d 385, 389 (6th Cir. 1977) ("the district court had authority under the All Writs Act, 28 U.S.C. § 1651(a), to require the telephone company to provide the necessary assistance for the tracing of calls"); *cf. United States v. Illinois Bell Tel. Co.,* 531 F.2d 809, 814 (7th Cir. 1976) ("analogous

authority for the proposition that the telephone company cannot frustrate the exercise of the district court's order by refusing to make available its facilities and know-how, is the All Writs Act").

The same concerns that motivated the use of the All Writs Act in the pen register cases apply here, as well. The Supreme Court was concerned that "without the Company's assistance there is no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished." *New York Tel. Co.,* 434 U.S. at 175. So, too, with the warrants issued by this Court: barring a triumph in cryptanalysis, without Fricosu's assistance, there is no conceivable way in which the search authorized by this Court could be successfully accomplished. Just as the Court may use its authority to ensure that grand jury subpoenas are not frustrated, *see Shillitani v. United States,* 384 U.S. 364, 370-71 (1966), it also may use its authority under the All Writs Act to ensure that search warrants are not frustrated.

B. The Application seeks the decrypted contents of the computer, not information from Ms. Friscou's head

Ms. Fricosu's opposes the Application by characterizing it as requesting an invasion into her mind. She states that the Application would demand a "key" that is "in Ms. Fricosu's head," (Doc. 174 at 3), analogizing it directly to the "compelled disclosure of a safe's combination." To the contrary, the applied-for order would not give the government access to anything "in Ms. Fricosu's head," (Doc. 174 at 3); nor would it require Fricosu to "disclose" anything "that exists in her mind," (Doc. 172-1 at 6). It does not require her to disclose the key to the government, or to anyone else. The Application requires only that Fricosu "make available the unencrypted contents of the

Subject Computer." (Doc. 111 at 2). As of today, the government does not know the encryption key. Should the Court grant the order, the government still would not know the encryption key. Ms. Fricosu argues that the proposed order is closer to "the compelled disclosure of a safe's combination" than it is to her being "forced only to provide 'the key to a strongbox.'" (Doc. 174 at 3). To the contrary, the government seeks the strongbox's contents, not the ability to open the strongbox for itself.

While Ms. Fricosu describes this Application as unprecedented, (Doc. 174 at 4), Amicus Electronic Frontier Foundation describes the Application as containing an "aggressive argument" with "far-reaching consequences." (Doc. 172-1 at 1). The Fifth Amendment privilege against self-incrimination is not a privilege against disclosing data in an unencrypted format. For example, in a publication entitled "Know Your Rights!," the Electronic Frontier Foundation answered the question "If the police ask for my encryption keys or passwords, do I have to turn them over?," this way:

> **No.** The police can't force you to divulge anything. However, a judge or a grand jury may be able to. The Fifth Amendment protects you from being forced to give the government self-incriminating testimony. If turning over an encryption key or password triggers this right, not even a court can force you to divulge the information. But whether that right is triggered is a difficult question to answer. If turning over an encryption key or password will reveal to the government information it does not have (such as demonstrating that you have control over files on a computer), there is a strong argument that the Fifth Amendment protects you. If, however, turning over passwords and encryption keys will not incriminate you, then the Fifth Amendment does not protect you. ***Moreover, even if you have a Fifth Amendment right that protects your encryption keys or passwords, a grand jury or judge may still order you to disclose your data in an unencrypted format under certain circumstances.*** If you find yourself in a situation where the police are demanding that you turn over encryption keys or passwords, let EFF know.

Hanni Fakhoury, *Know Your Rights!*, ELECTRONIC FRONTIER FOUNDATION 2-3

(June 2011), https://www.eff.org/files/EFF_Know_Your_Rights_2011.pdf (footnotes removed; bold italics added).

This Application falls exactly into that latter category: It does not require Ms. Fricosu to turn over an encryption key, or to "disclose" or testify to anything. The proposed order would require the production of data in an unencrypted format. EFF's "Know Your Rights!" publication correctly states that a judge may properly order the production of unencrypted data consistent with the Fifth Amendment.

C. The Fifth Amendment privilege against self-incrimination does not apply to the production of voluntarily created, pre-existing documents

Amicus, though not Ms. Fricosu, argues that "the fact the witness might type the information into a keyboard rather than speak it aloud" makes no difference. (Doc. 172-1 at 7). But the Supreme Court has, to the contrary, attached great importance to the distinction between a compelled ***communication*** and a compelled ***production*** of pre-existing documentary evidence.

The Fifth Amendment's protection against self-incrimination "applies only when the accused is compelled to make a testimonial ***communication*** that is incriminating." *Baltimore City Dept. of Social Services v. Bouknight,* 493 U.S. 549, 554 (1990) (emphasis added). A communication is testimonial when it "explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." *Id.* A communication is non-testimonial when a person is "not required 'to disclose any knowledge he might have,' or 'to speak his guilt.'" *United States v. Doe,* 487 U.S. 201, 210 (1988) (hereinafter, *Doe II*) (quoting *United States v. Wade,* 388 U.S. 218, 222-23 (1967)). However, the self-incrimination protection applies only to communications: "Unless some attempt is made

to secure a ***communication***—written, oral or otherwise—upon which reliance is to be placed as involving [the accused's] consciousness of the facts and the operations of his mind in expressing it, the demand made upon him is not a testimonial one." *Id.* (emphasis added).

Thus, "certain acts, though incriminating, are not within the privilege" against self-incrimination, because they are not communications at all. *Id*. These include furnishing a blood sample, providing a handwriting exemplar, providing a voice exemplar, standing in a lineup, wearing particular clothing, *id.* (citing cases), and producing a child in response to a court order, *see Bouknight,* 493 U.S. at 559.

The Supreme Court has also treated the compelled production of pre-existing, voluntarily created documents as a non-testimonial act—except to the extent that the act of producing the documents might incriminate the defendant, an issue dealt with below. *See United States v. Doe,* 465 U.S. 605, 611-612 (1984) (hereinafter, *Doe I*). *Doe I* involved grand jury subpoenas served on the owner of several small proprietorships, demanding the production of business records. The subpoena recipient moved to quash under the Fifth Amendment, arguing that the contents of the records could incriminate him. The Supreme Court rejected that argument, holding that so long as a defendant "does not contend that he prepared the documents involuntarily or that the subpoena would force him to restate, repeat, or affirm the truth of their contents," then "the contents of those records are not privileged." *Id.* at 611-12; *see also In re Foster,* 188 F.3d 1259, 1269 (10th Cir. 1999). Ms. Fricosu does not claim that she saved files to her hard drive involuntarily. The applied-for order also does not

require her to "restate, repeat, or affirm the truth of" any statements in those files. Thus, requiring her to produce decrypted data is consistent with the Fifth Amendment.

The Court is on even safer Fifth Amendment ground here, because the government has obtained the evidence through a search warrant, not a grand jury subpoena. Evidence obtained through search warrants does not implicate the self-incrimination clause because search warrants do not compel individuals to make statements. In *Andresen v. Maryland,* 427 U.S. 463 (1976), the Supreme Court considered whether the search of the defendant's offices for business records, their seizure, and subsequent introduction into evidence violated the Fifth Amendment. The court held that the Fifth Amendment did not apply, because the defendant "was not asked to say or to do anything. The records seized contained statements that petitioner had voluntarily committed to writing." *Id.* at 473; *see also Fisher,* 425 U.S. at 407-408 ("any notion that 'testimonial' evidence may never be seized and used in evidence is inconsistent with" cases upholding wiretaps). Here, too, the applied-for order would use as the source of evidence only material seized with a warrant; it would not make use of any compelled statements.

D. Ms. Fricosu's act of producing the unencrypted hard drive contents would not incriminate her, especially given the proposed act-of-production immunity

In limited circumstances, the act of turning over a document could inherently communicate incriminating facts and thus be protected by the Fifth Amendment. *United States v. Hubbell,* 530 U.S. 27, 40-41 (2000). "[T]he testimonial aspect of a response to a subpoena duces tecum does nothing more than establish the existence,

authenticity, and custody of items that are produced." *Id.* However, when the "existence and location" of documents under a subpoena are a "foregone conclusion" and the witness "adds little or nothing to the sum total of the Government's information" by conceding he has them, the privilege against self-incrimination does not apply. *United States v. Fisher,* 425 U.S. 391, 411 (1976). That is the case here.

1. Ms. Fricosu's production of the unencrypted documents would not be a testimonial act of production

Ms. Fricosu argues that complying with the order would be a testimonial act of production, because "the existence and location of incriminating evidence on the encrypted hard drive are not a foregone conclusion;" moreover, she argues that "the government does not know that the computer belongs to or was used by Ms. Fricosu or that she had or has access to the drive." (Doc. 174 at 3). Both her premises and conclusions are wrong.

Her premises are wrong because, as explained in the Application, the government ***does*** have evidence showing to whom the Subject Computer belongs and what it contains: the Subject Computer "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." (Doc. 111 at 5).

Yet even if the government were ignorant of these facts, Ms. Fricosu's argument still fails because she confuses what the government could learn from the act of

production with what the government could learn from the ***contents*** of what is produced. The act of production is privileged, *see Doe I,* 465 U.S. at 612, but the contents of production are not, *see id.* at 610-12; *United States v. Hubbell,* 530 U.S. 27, 40 (2000) ("The 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents."); *In re Foster,*188 F.3d 1259, 1269 (10th Cir. 1999) ("The Fifth Amendment does not shield from discovery the contents of any documents Foster voluntarily created, even if the contents incriminate him."). Both Ms. Fricosu and Amicus erroneously focus their "foregone conclusion" analysis on the contents of the documents produced, rather than on the act of producing them. While conclusions the government might draw from the ***contents*** of the laptop certainly are not foregone, the limited conclusions that the government might draw from Ms. Fricosu's ***producing*** those contents are foregone. An act of production might reveal "the existence, authenticity, and custody of items," *Hubbell* at 40, but the existence, authenticity, and custody of the decrypted data are already foregone conclusions because the government possesses the laptop, having seized it with a lawful search warrant, and already has ample evidence linking Ms. Fricosu to the laptop. Thus, the government knows the data exists, and knows where it is.

If it were really the case that the government had to already know the contents of the evidence before the defendant produced it, (Doc. 174 at 4), then the act-of-production privilege would swallow the authority, recognized by the Supreme Court, to compel the production of pre-existing voluntarily created incriminatory

evidence. *See Doe I,* 465 U.S. at 611-612; *United States v. Fisher,* 425 U.S. 391 (1976). This is also exactly the reasoning rejected by the district court in *In re Boucher,* 2009 WL 424718 (D. Vt. 2009). There, the court clarified that the existence, location, and authenticity of the contents of an encrypted drive in the government's possession were foregone conclusions. *Id.* at *3-*4. This was so because the government "knows of the existence and location of the [encrypted] drive and its files." *Id.* at 3. Although that knowledge in *Boucher* was additionally confirmed by an officer's "view[ing] the contents of some of the [encrypted] drive's files," *id.*, the *Boucher* court pointedly did not rely on the fact, instead noting that "Second Circuit precedent, however, does not require that the government be aware of the incriminatory *contents* of the files; it requires the government to demonstrate 'with reasonable particularity that it knows of the existence and location of subpoenaed documents.'" *Id.* at *3 (*quoting In re Grand Jury Subpoena,* 1 F.3d 87, 93 (2d Cir. 1993)). *Boucher* sets a standard that is met here. The government knows the "existence" of decrypted data, because it knows of the existence of ***encrypted*** data, and the one is generated from the other. The government knows the "location" of decrypted data, because the laptop's location is known. The act of producing the contents of that encrypted drive would, therefore, merely be cumulative evidence that would support what the government already knows—in other words, it would support foregone conclusions.

The requirement that Ms. Fricosu produce *all* of the encrypted laptop distinguishes this case from *United States v. Hubbell,* 530 U.S. 27 (2000). In *Hubbell,* the Supreme Court held that a defendant's assembly of documents in response to a

grand jury subpoena violated his privilege against self-incrimination. The Court held that the subpoena required not just documents, but "respondent's assistance both to identify potential sources of information and to produce those sources." *Id.* at 41. This was "tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions," *id.;* hence, "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena," *id.* at 43. By comparison, the applied-for order here would not require Fricosu to select responsive documents, or answer anything resembling an interrogatory; it requires her to provide the entire contents of a single hard drive, particularly described in a search warrant approved by a detached and neutral magistrate. While Ms. Fricosu might use the contents of her mind in the course of complying (as would, for example, "an accused… required to submit a handwriting exemplar," *Fisher,* 425 U.S. at 411) the order would not require her to disclose those contents.

Amicus (although not Ms. Fricosu) additionally argues that Ms. Fricosu's act of producing the decrypted hard drive would incriminate her because "The act would be an admission that she had control over the computer and the data stored on it before it was seized from her residence." (Doc. 172-1 at 7). But custody and control were foregone conclusions: an agent executing a search warrant found the computer not only in Ms. Fricosu's home, but on the floor of her personal bedroom. Additionally, 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. Hence, it is a foregone conclusion that Ms. Fricosu had sufficient control over the computer to decrypt and use it.

2. The grant of act-of-production immunity would, alternatively, satisfy the act-of-production privilege

Even if the Court were to conclude that producing the contents of the decrypted drive would be a testimonial act of production, the United States has, with its application, asked the court to grant Ms. Fricosu act-of-production immunity. Consistent with that immunity grant, Ms. Fricosu's acts of decrypting the drive and making its contents available could not "be used against [her] in any criminal case." 18 U.S.C. § 6002. Thus, even to the extent that her act of decrypting the hard drive might demonstrate that she had control over it, or that its contents were authentic, the United States would be prohibited from using that act-of-production evidence at trial. Consequently, Ms. Fricosu may not withhold the act-of-production on Fifth Amendment grounds. *See Kastigar v. United States,* 406 U.S. 441 (1972).

The immunity would also prevent the government from using "evidence derived directly and indirectly" from the act of production. *Id.* at 453; *see also* 18 U.S.C. § 6002. Ms. Fricosu argues that this means she must be given immunity "preventing the government's use of incriminating information derived… from the compelled decryption of the hard drive." (Doc. 174 at 4). Amicus, similarly, seems to characterize the decrypted contents of the hard drive as evidence "derived" from the act of production. Ms. Fricosu and Amicus again confuse the act of production with the contents of what is

produced. Their argument is inconsistent with Supreme Court cases holding that the Fifth Amendment permits the government to subpoena pre-existing evidence from both defendants and third parties. *See Baltimore City Dept. of Social Services v. Bouknight,* 493 U.S. 549, 554 (1990); *United States v. Doe,* 465 U.S. 605, 611-612 (1984); *United States v. Fisher,* 425 U.S. 391 (1976). Had the Supreme Court believed the contents of those productions were all "derived" from the acts of producing them, those cases would have been decided differently. Under those cases, should the Court grant the Application, then the decrypted contents of Ms. Fricosu's laptop would not be information impermissibly "derived" from a testimonial act of production—just as the contents of paper business records are not information impermissibly "derived" from the act of their production, and facts learned from a handwriting exemplar are not impermissibly "derived" from the act of producing the exemplar.

E. The privilege against self-incrimination must be interpreted narrowly and is not a mechanism to protect abstract privacy

Ms. Fricosu asks for a "liberal construction" of the self-incrimination clause, (Doc. 174 at 4), and Amicus similarly asks the court to decide the legal question presented "in a way that recognizes the substantial benefits of encryption to safeguard the security and privacy of digital information stored on computers," (Doc. 172-1 at 13). But the Supreme Court has specifically cautioned against expansive readings of the self-incrimination clause: all privileges are "exceptions to the demand for every man's evidence." *United States v. Nixon,* 418 U.S. 683, 710 (1974). Because privileges deprive the justice system of truthful evidence, the Court has cautioned that they should

be "not lightly created nor expansively construed, for they are in derogation of the search for truth." *Id.*

That encryption has "substantial benefits" does not mean that courts should never require individuals to produce decrypted data. The government seeks this application in connection with a search warrant, and relies upon the court's discretion under the All Writs Act to compel Ms. Fricosu to produce decrypted data. This Application occurs only after a thorough investigation, supported by probable cause, and intermediated by a judicial officer at two different points (the warrant and the All Writs Act application). Granting the application, then, will not dissuade responsible individuals from using encryption to safeguard trade secrets or sensitive customer information; it is understood that this type of order is, like a search warrant, an event that occurs only when "the individual's interest in privacy must give way to the magistrate's official determination of probable cause." *United States v. Ross,* 456 U.S. 798, 823 (1982). Granting the application would, however, recognize law enforcement's legitimate needs to obtain evidence with search warrants—needs that encryption would otherwise thwart.

Moreover, the Supreme Court has cautioned that the Fifth Amendment's self-incrimination clause is not a vehicle to protect abstract privacy. The Framers "addressed the subject of personal privacy directly in the Fourth Amendment," but "did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination." *Fisher,* 425 U.S. at 400. While the prospect of subjecting a hard drive to forensic examination unquestionably implicates privacy concerns, those concerns were addressed when the

government obtained search warrants. The question presented by this Application is whether Ms. Fricosu may frustrate those warrants.

CONCLUSION

The government requests the application be granted.

Respectfully submitted this 18th day of July, 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: 303/454-0403
patricia.davies@usdoj.gov

s/Jeremy Sibert
JEREMY SIBERT
Assistant United States Attorney
1225 Seventeenth Street, Suite 700
Denver, Colorado 80202
Telephone: (303) 454-0100
Facsimile: (303) 454-0406
E-mail: Jeremy.Sibert@usdoj.gov

Attorneys for Government

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of July, 2011, I electronically filed the foregoing **GOVERNMENT'S REPLY TO AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT FRICOSU'S OPPOSITION TO GOVERNMENT'S APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS (Docket #172-1) and MS. FRICOSU'S RESPONSE TO DOCUMENT 111 (Docket #174)** with the clerk of the Court using the CM/ECF system which will send notification of such filing to the following email addresses:

Tonya Shotwell Andrews
Tonya.Andrews@usdoj.gov,judith.harding@usdoj.gov,raisa.pitman@usdoj.gov,pamela.thompson3@usdoj.gov,michelle.lockman@usdoj.gov,nicole.davidson@usdoj.gov,usaco.ecfcivil@usdoj.gov,pam.jebens@usdoj.gov

Patricia W. Davies
patricia.davies@usdoj.gov,USACO.ECFCriminal@usdoj.gov,veronica.ortiz@usdoj.gov

Philip L. Dubois
dubois@dubois.com,phil_dubois2000@yahoo.com

Hanni Meena Fakhoury
hanni@eff.org,steph@eff.org

Marcia Clare Hofmann
marcia@eff.org,steph@eff.org

Mark Cameron Johnson
mark.johnson68@gmail.com

Martha Ann Paluch
Martha.Paluch@usdoj.gov,judith.harding@usdoj.gov,pamela.thompson3@usdoj.gov,nicole.davidson@usdoj.gov,raisa.pitman@usdoj.gov,ma-linda.la-follette@usdoj.gov,michelle.lockman@usdoj.gov,USACO.ECFCivil@usdoj.gov,pam.jebens@usdoj.gov

s/Valerie Nielsen
VALERIE NIELSEN
Legal Assistant
U.S. Attorney's Office
1225 Seventeenth Street, Suite 700
Denver, Colorado 80202
Telephone: (303) 454-0100
Fax: (303) 454-0406
E-mail: valerie.nielsen@usdoj.gov