UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Judge Robert E. Blackburn

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

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. RAMONA CAMELIA FRICOSU,

Defendant.

BRIEF OF AMICUS CURIAE 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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTE

CONSTITUTIONAL AMENDMENT

STATEMENT OF INTEREST OF AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization. As part of its mission, EFF has served as counsel or amicus in key cases addressing user rights to privacy, free speech, and innovation as applied to the Internet and other new technologies. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

EFF's interest in this case is the sound and principled application of the Fifth Amendment to encryption passwords and encrypted information stored on computers. Encryption is a widely used and fundamental safeguard for businesses and individuals who store data on portable devices like laptops, which may be easily lost or stolen. EFF submits this brief to help the Court apply the Fifth Amendment privilege against self-incrimination in a manner that ensures the constitutional rights of those who use this technological measure to protect their privacy and security.

INTRODUCTION

The government seeks to force defendant Ramona Fricosu to enter a password into a laptop or otherwise provide access to encrypted data stored on that computer. The government hopes this information will include evidence of allegedly criminal activity it can use to prosecute this case.

The Court should reject the government's application because it is contrary to the Constitution, long-standing Supreme Court precedent, and sound public policy. The government makes an aggressive argument here that may have far-reaching consequences for all encryption users. Fricosu will be made a witness against herself if

she is forced to supply information that will give prosecutors access to files they speculate will be helpful to their case but cannot identify with any specificity. And while Fricosu has been offered limited immunity, it is not enough to defeat her Fifth Amendment privilege against self-incrimination.

FACTUAL BACKGROUND

A. Statement of Relevant Facts

The government has indicted defendants Ramona Fricosu and Scott Whatcott on various charges arising from allegedly fraudulent real estate transactions. (Dkt. 1.) On May 14, 2010, the government executed search warrants at the residence that Fricosu shares with her mother and two children, and formerly shared with her co-defendant Scott Whatcott. The government seized, among other items, several computers and storage devices containing digital information. One of the seized computers was a Toshiba Satellite M305 laptop. The government obtained an additional search warrant to search this laptop, but discovered that it was unable to read the encrypted contents of the computer.

On May 6, 2011, the government filed an application under the All Writs Act, 28 U.S.C. § 1651, asking the Court to compel Fricosu to type her encryption password into the laptop. (Dkt. 111.) Specifically, the government contends, "Ms. Fricosu could enter the password without being observed by the government, or otherwise provide the unencrypted contents of the [laptop] by means she chose." Gov. App. at 2-3.

B. Encryption is an Important Measure to Protect Security and Privacy

Encryption is a process by which a person can change plain, understandable information into unreadable letters and numbers using a mathematical algorithm. Only someone with a special code—an encryption key or password—is able to decipher the

information to make it readable again.[1] Computer and software manufacturers consider disk encryption a basic computer security measure and include disk encryption tools as a standard feature on most new computers.[2] Among other things, encryption is extremely useful for protecting information on small, portable devices like laptops, which can easily be stolen or lost.[3] Typically, encryption protects sensitive information on these devices from unauthorized access, even if a lost or stolen device is never recovered. Encryption helps to ensure that data is not misused if it falls into the wrong hands.

Encryption is increasingly recognized as a critical way for companies to secure

---

[1] *See generally* Encryption, https://secure.wikimedia.org/wikipedia/en/w/index.php?title=Encryption&oldid=433989373 (last visited July 8, 2011).

[2] For example, the Microsoft Windows operating system has come with the Bitlocker Drive Encryption feature since 2008. *See, e.g.,* Microsoft, Bitlocker Drive Encryption Overview, http://technet.microsoft.com/en-us/library/cc732774.aspx (last visited July 7, 2011). The four most recent versions of Apple's Mac OS X 10 operating system have included FileVault, which is a program that allows users to encrypt files in their home folder. FileVault, https://secure.wikimedia.org/wikipedia/en/w/index.php?title=FileVault&oldid=437137960 (last visited July 8, 2011). The company plans to introduce a more sophisticated full-disk encryption feature in a new OS release later this month. Apple Insider, *Inside Mac OS X 10.7 Lion: FileVault Full Disk Encryption and Cloud Key Storage* (Feb. 28, 2011), http://www.appleinsider.com/articles/11/02/28/inside_mac_os_x_10_7_lion_file_vault_full_disk_encryption_and_cloud_key_storage.html.

[3] *See, e.g.,* Rich Phillips, *BP Loses Laptop With Private Info on 13,000 People,* CNN.com (March 29, 2011), http://articles.cnn.com/2011-03-29/us/bp.lost.laptop_1_deepwater-horizon-oil-spill-laptop?_s=PM:US; Neil Versel, *VA Laptop Incidents Show Why Encryption Is So Important*, Fierce Mobile Health Care, (Sept. 21, 2010) http://www.fiercemobilehealthcare.com/story/latest-va-laptop-incidents-show-why-encryption-so-important/2010-09-21; Paul McNamera, *Latest "Lost" Laptop Holds Treasure-Trove of Unencrypted AT&T Payroll Data*, Network World (June 5, 2008), http://www.networkworld.com/community/node/28453; Bob Sullivan, *Lost IRS Laptop Stored Employee Fingerprints*, MSNBC.com (June 5, 2006), http://www.msnbc.msn.com/id/13152636/ns/technology_and_sciencesecurity/t/lost-irs-laptop-stored-employee-fingerprints/; Robert Ellis Smith, *Laptop Hall of Shame*, Forbes.com (Sept. 7, 2006), http://www.forbes.com/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html.

data on their computers, which can range from proprietary business information like trade secrets to sensitive customer information like credit card numbers. According to a 2010 study by Intel and the Ponemon Institute, 329 public and private organizations collectively reported more than 86,000 laptops stolen or missing over a 12-month period—an average of 263 laptops per organization. *The Billion Dollar Lost Laptop Problem* at 1 (Sept. 30, 2010).[4] Forty-six percent of those organizations said that they lost laptops with sensitive or confidential information, while 30 percent of the lost laptops had full-disk encryption. *Id*. at 6. Intrusions into computers by outsiders have also put unencrypted personal information at risk.[5] It is therefore not surprising that an increasing number of businesses consider full-disk encryption a priority,[6] which means that more and more employees encrypt the contents of their work computers.[7]

Encryption also provides critical protection for data stored on individuals' personal computers. People keep vast amounts of information on their digital devices, which might include years of correspondence with friends, family members, and colleagues; personal photographs and videos; Internet browsing histories; financial

[4] Available at http://newsroom.intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf.

[5] *See*, *e.g.*, Reuters, *Thousands of Citi Customers at Risk After Hacker Attack* (June 9, 2011), http://www.msnbc.msn.com/id/43335996/ns/business-personal_finance/t/thousands-citi-customers-risk-after-hacker-attack; Jason Schreier, *Sony Hacked Again; 25 Million Entertainment Users' Info at Risk*, Wired.com (May 2, 2011), http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack.

[6] *New DigitalPersona Survey Shows SMBs Consider Disk Encryption a Priority*, Small Business Trends, (June 25, 2011) http://smallbiztrends.com/2011/06/survey-smbs-disk-encryption.html.

[7] Indeed, several states now encourage or even require businesses to use encryption to safeguard information they collect. Colorado law, for example, requires companies to notify state residents when their unencrypted personal data has been compromised and possibly misused. C.R.S. 6-1-716. Massachusetts has taken an even stronger stance, requiring everyone who owns or licenses personal data about state residents to encrypt all personal data stored on laptops and portable storage devices. *See* Mass. General Law Chapter 93H and regulations promulgated by the Office of Consumer Affairs and Business Regulation at 201 CMR 17.00.

information; sensitive medical details; and confidential work-related information. People may carry this data with them every day on laptops, tablets, and phones that could be left behind in a taxi, stolen at a café, or inspected by a prying acquaintance.

As businesses and individuals alike recognize the need to protect the privacy and security of the information on their computers, more and more people will find themselves in Fricosu's situation: facing a government attempt to force them to turn over an encryption password or a decrypted version of the data stored on a computer. Very few courts have considered whether such compulsion violates the Fifth Amendment privilege against self-incrimination. The Court should address this question with deliberation and care because it involves fundamental constitutional rights.

ARGUMENT

The Fifth Amendment provides that "no person . . . shall be compelled in any criminal case to be a witness against himself[.]" U.S. CONST. AMEND. V. Not surprisingly, the few courts to consider the question have found that this right prevents the government from forcing a witness to testify to a password used to restrict access to files on a computer. *United States v. Rogozin*, 09-CR-379, 2010 WL 4628520 at **5-6 (W.D.N.Y. Nov. 16, 2010); *United States v. Kirschner*, No. 09-MC-50872, 2010 WL 1257355 at **3-4 (E.D. Mich. March 30, 2010).

This case presents a slightly different question, which is whether the government can compel a witness to type a password into a laptop or otherwise provide access to encrypted data stored on that computer. *See In re Grand Jury Subpoena to Sebastien Boucher*, 2:06-mj-91, 2007 WL 4246473 at *6 (D. Vt. Nov. 29, 2007) (*Boucher I*), *appeal sustained by* 2009 WL 424718 (D. Vt. Feb. 29, 2009) (*Boucher II*). Under the circumstances of this case, the answer is no.

Decrypting data on a computer is a testimonial act that receives the full

protection of the Fifth Amendment. This act would incriminate Fricosu because it might reveal she had control over the laptop and the data there. The government has failed to show that the existence and location of the information it seeks is a foregone conclusion. Furthermore, the limited immunity offered by the government is not coextensive with the scope of Fricosu's privilege. The Court should therefore find that the government has failed to take the steps necessary to secure Fricosu's Fifth Amendment rights and deny the application.

A. The Act of Entering a Password or Otherwise Decrypting Data on a Computer is a Compelled Testimonial Act Protected By The Fifth Amendment.

The Fifth Amendment generally protects a person from being compelled to give testimony that would incriminate her. *United States v. Hubbell*, 530 U.S. 27, 34 (2000) (*Hubbell I*); *Fisher v. United States*, 425 U.S. 391, 408 (1976). The privilege is limited to testimonial evidence, or a communication that "itself, explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." *Doe v. United States*, 487 U.S. 201, 210 (1988) (*Doe I*). Put a different way, the privilege protects the "expression of the contents of an individual's mind." *Id*. at 210 n.9; *see also* 220 n.1 (Stevens, J., dissenting). To illustrate this principle, the Supreme Court has explained that a witness might be "forced to surrender a key to a strongbox containing incriminating documents," but not "compelled to reveal the combination to a wall safe." *Id.* at 210 n.9; *see also* 219 (Stevens, J., dissenting). Forcing an individual to supply a password necessary to decrypt data is more like revealing the combination to a wall safe than to surrender a key: the witness is being compelled to disclose information that exists in her mind, not to hand over a physical item. *Boucher I*, 2007 WL 4246473 at *4.[8]

[8] Despite the fact that *Boucher II* sustained the government's appeal of *Boucher I*, the earlier decision was well reasoned and is worth consideration. In that case, a grand jury issued a subpoena to compel the defendant to enter a password to allow the government access to encrypted files on a particular drive on a computer. 2007 WL

The fact that the witness might type the information into a keyboard rather than speak it out loud does not change that basic fact. The act of disclosing information may be so testimonial that the privilege applies to the production itself. *United States v. Doe*, 465 U.S. 605 (1984) (*Doe II*). An act of production has a sufficiently testimonial aspect to trigger Fifth Amendment protection when it forces a witness to admit the existence of papers, the fact that they were in her possession or control, and that they were authentic. *Hubbell I*, 530 U.S. at 36 (citing *Doe II*, 465 U.S. at 613 (internal quotation marks omitted)).

Forcing Fricosu to enter the laptop password into the computer or otherwise decrypt the data stored on the computer meets this standard because the act of doing so will imply assertions of fact. *See Hubbell I*, 530 U.S. at 37. 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—which are critical admissions, particularly considering that she shared her residence with her co-defendant. The act would also show that she knows the encryption password and was able to access the encrypted data. If Fricosu knows the password, forcing her to perform the act of decrypting the data on the laptop will put her in the "cruel trilemma" that the privilege is designed to protect against:

4246473 at *1. A magistrate judge determined that entry of the password was a testimonial act with which the government's grant of immunity was not coextensive, and the foregone conclusion doctrine did not apply. *Id*. at **3-6. The government subsequently modified the subpoena so that it did not seek to force the defendant to turn over his password, but instead provide the grand jury a decrypted version of the contents of the drive. *Boucher II,* 2009 WL 424718 at *1. The court upheld the subpoena as modified, finding that the defendant had no privilege to refuse to turn over the decrypted data because the government already knew of the existence and location of the files at issue. *Id*. at *4. Thus, *Boucher II* analyzed a different request for information than *Boucher I*, and while the defendant's motion to quash the modified subpoena was ultimately denied and the government's appeal sustained, most of *Boucher I*'s analysis was not overruled by *Boucher II* (but see footnote 9 *infra)*.

having to choose between incriminating herself, lying under oath, or refusing to answer and risking contempt of court. *Doe I*, 487 U.S. at 212; *Boucher I*, 2007 WL 4246473 at *3.

Even if the act were not so directly incriminating, the privilege applies not only where an act of production would itself incriminate a witness, but also to an act "which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hubbell I*, 530 U.S. at 38 (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951) (internal quotation marks omitted)). It appears undisputed that the encrypted data the government hopes to access might incriminate Fricosu. Gov. App. at 4. This is a vital consideration where she has been indicted on more than 30 counts since the government seized the laptop, regardless of the fact that the government has agreed not to use the act of producing the decrypted data against her. As explained below, this immunity offer is inadequate under the circumstances of this case.

B. Neither the Encryption Password Nor the Decrypted Contents of the Laptop Is a Foregone Conclusion.

The government contends that the existence and location of the decrypted contents of the laptop are a forgone conclusion because incriminating evidence might be found there. Gov. App. at 7 & 9. This argument misconstrues the foregone conclusion doctrine in a dangerous way, and the Court should not accept this interpretation of the law.

When the existence and location of information are known to the government, and the witness "adds little or nothing to the sum total of the Government's information by conceding that [s]he in fact has the [information]," those matters are treated as a "foregone conclusion." *Fisher*, 425 U.S. at 411. Under those circumstances, "no constitutional rights are touched. The question is not of testimony but of surrender." *Id*. citing *In re Harris*, 221 U.S. 274, 279 (1911). In situations where the foregone

conclusion doctrine applies, the government typically already has extensive information about the material it seeks. *United States v. Hubbell*, 167 F.3d 552, 576 (D.C. Cir. 1999) (*Hubbell II*), *aff'd Hubbell I*, 530 U.S. 27. The government's knowledge of the existence, control, location and authenticity of the information must be nearly the same as the witness's for the doctrine to overcome the privilege. *Id*. at 576-78.

The government has not made that showing here. It claims that the laptop "has a very high likelihood of containing evidence pertaining to the charged crimes," Gov. App. at 7, that the "charged offenses were facilitated substantially by computers," Gov. App. at 4, and that other digital storage devices seized from the home Fricosu shared with Whatcott contained documents relating to the charged offenses, Gov. App. at 4-5. But a "very high likelihood" is nothing more than an educated guess. The government can identify neither specific evidence it expects to find on this particular laptop, nor where this supposed evidence might be found on the computer. This is not a situation in which the password will "add[] little or nothing to the sum total of the Government's information[.]" *Fisher*, 425 U.S. at 411. To the contrary, compelling Fricosu to supply the information will add a great deal to the government's knowledge that it does not already have.

Only one case has addressed a similar legal question, and the facts here are so different that they require a different result.[9] *Boucher II* considered whether the defendant could be forced to turn over a decrypted version of data stored in a particular drive on a laptop. 2009 WL 424718 at **1-2. In that case, the defendant had already acknowledged to the government that he owned the computer. *Id*. at *1. He had displayed the contents of some of the files, revealing that they likely included images or videos of child pornography. *Id*. at **1-2. The government independently searched for

[9] To the extent that *Boucher II* overrules *Boucher I*, it is likely on this question. *Boucher II*, 2009 WL 424718 at **3-4.

and located files they suspected were child pornography. *Id*. at *2. The defendant also accessed a particular drive on the computer in a government agent's presence, where the agent located and examined several files that appeared to be contraband. *Id*. Under the circumstances, the court concluded that providing the government access again to the files on the drive "add[ed] little or nothing to the sum total of the Government's information about the existence and location of files that may contain incriminating information," and was therefore a foregone conclusion. *Id.* at *3 (citing *Fisher*, 425 U.S. at 411) (internal quotation marks omitted).

Unlike the investigators in *Boucher II*, government agents here have never viewed any data on the laptop. The government contends that Fricosu discussed a laptop with Whatcott in taped conversations, Gov. App. at 5, but has not shown that the laptop seized from the residence is the same laptop mentioned in these discussions. Even assuming the government could show that it is the same laptop, it can identify neither files relevant to this investigation nor their location on the computer.[10]

The facts of this case are more like those in *Hubbell I*. In that case, the government issued a subpoena ordering the defendant to produce eleven categories of documents, which the defendant had to help produce. 530 U.S. at 41. Noting that the government could independently prove neither the existence nor the whereabouts of the documents produced in response to the subpoena, the Court rejected the argument that the papers' existence and location were a foregone conclusion. 530 U.S. at 44-45. In particular:

[10] To the extent the government seeks to force Fricosu to type a password into the computer, as *Boucher I* notes, the foregone conclusion doctrine likely does not apply. 2007 WL 4246473 at *6. Assuming Fricosu has no written record of the password, it exists only in her mind (if she knows it at all). Compelling her to type the information into a computer "is pure testimonial production rather than physical evidence having testimonial aspects," and the foregone conclusion document would not come into play. *Id*.

> The documents did not magically appear in the prosecutor's office like "manna from heaven." They arrived there only after [the defendant] . . . took the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the . . . potentially incriminating evidence sought by the subpoena.

Id. at 42. So too is the case here. What the government might find on the laptop is not a foregone conclusion, but only will be available to the government if Fricosu can supply the information necessary to produce a decrypted version of the data.

The government suggests that this case is analogous to *Fisher* and *Doe I*. Gov. App. at 8. But those cases are easily distinguishable on the facts. In *Fisher*, the government was able to confirm the existence and authenticity of subpoenaed documents through an independent third party who also possessed copies of them. 425 U.S. at 402. As the Supreme Court explained, "[C]ompelled production of documents from an attorney does not implicate whatever Fifth Amendment privilege the taxpayer might have enjoyed from being compelled to produce them *himself*." *Id*. (emphasis added). Here, there is no indication that an independent third party can provide the information sought. And in *Doe I*, the Supreme Court found that it was constitutional to compel a witness to sign a consent directive that did not confirm the existence of a specific foreign bank account or authenticate any records that might be in the possession of a foreign bank. 487 U.S. at 215-16. In contrast, forcing Fricosu to provide the information necessary to decrypt the data on the laptop will directly link her to the computer and the data on it.

C. Limited "Act of Production" Immunity is Not Coextensive With Fricosu's Fifth Amendment Privilege Unless It Extends to Evidence on the Laptop Derived From Disclosure of the Password.

The government seeks the Court's approval to grant Fricosu "limited immunity" to prevent the government from using the act of producing the unencrypted data against her in any prosecution. Gov. App. at 7-8. Specifically, this immunity will not permit the

government to use the *act* of production against Fricosu, but apparently will allow the government to use the data actually obtained through the act of production against her, as well as any evidence the government learns as a result of accessing that information. This limited immunity does not defeat Fricosu's Fifth Amendment privilege against self-incrimination because it is not "coextensive with the scope of the privilege." *Kastigar v. United States*, 406 U.S. 441, 453 (1972); *Boucher I*, 2007 WL 4246473 at *5.

When a witness's act of production is testimonial in character, the government must grant use and derivative-use immunity to satisfy the Constitution's requirements. *Hubbell I*, 530 U.S. at 41-46. This means that the government may not use the act of production itself against Fricosu, nor any evidence on the computer derived from the act of production. *Kastigar,* 406 U.S. at 453. As the Supreme Court has explained, use and derivative-use immunity "prohibits the prosecutorial authorities from using the compelled testimony in *any* respect, and it therefore insures that the testimony cannot lead to the infliction of criminal penalties on the witness." *Id*. (emphasis original).

Should the Court decide that Fricosu must supply the data on the laptop in decrypted form, the government will face a "heavy burden of proving that all of the evidence it proposes to use [from the laptop] was derived from legitimate independent sources." *Id*. at 461-62. Placing this burden on the government ensures that the grant of immunity leaves the prosecutors and witness "in substantially the same position as if the witness had claimed [her] privilege in the absence of a grant of immunity." *Hubbell I*, 503 U.S. at 40, citing *Kastigar*, 406 U.S. at 458-59 (internal quotation marks omitted).

The government's offer of limited immunity—with no guarantee against use or derivative use of the information Fricosu would be forced to supply—is not comprehensive enough to secure Fricosu's Fifth Amendment rights. She is therefore justified in refusing to provide the password. *Kastigar*, 406 U.S. at 449.

CONCLUSION

The government is overreaching to try to compel Fricosu to supply an encryption password that they hope will give them access to the full contents of a laptop. The Court should decide this important constitutional question in a way that recognizes the substantial benefits of encryption to safeguard the security and privacy of digital information stored on computers. New technologies present new challenges for law enforcement, but this reality does not justify the abandonment of well-established constitutional protections that secure individuals' rights. Decrypting data is an act with testimonial aspects that are protected by the Fifth Amendment. The government cannot identify the evidence it hopes to find with any specificity, and it has not offered Fricosu immunity coextensive with her Fifth Amendment privilege against self-incrimination. For all the reasons discussed above, the government's application should be denied.[11]

DATED: July 8, 2011

Respectfully submitted,

/s/ Marcia Hofmann
Marcia Hofmann (California Bar No. 250087)
Hanni Fakhoury (California Bar No. 252629)
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x. 116
Facsimile: (415) 436-9993
marcia@eff.org
hanni@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

[11] If the Court wishes to hear oral argument from EFF on the issues raised in this brief, undersigned counsel is happy to address any concerns or questions the Court may have. Counsel for EFF is unavailable on the July 22, 2011 hearing date currently scheduled for this motion, but would be willing to appear at a later date if convenient for the Court.