UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

Plaintiff,

v. Case No. 13-MJ-449-RTR

DECRYPTION OF A SEIZED
DATA STORAGE SYSTEM,

Defendant

AMICUS BRIEF IN SUPPORT OF REAL PARTY IN INTEREST JEFFREY FELDMAN'S OPPOSITION TO DECRYPTION

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Constitutional Provisions

INTRODUCTION

In an increasingly digital world, encryption is an essential means of safeguarding personal information from unwanted eyes. The tradeoff to using this technology, however, should not be a surrender of a person's Fifth Amendment right against compelled incriminating testimony when the government is unable to break decryption in a criminal investigation. For the reasons that follow, this Court should deny the government's writ and find that the Fifth Amendment protects Mr. Feldman from being forced to decrypt the storage devices.

STATEMENT OF FACTS

During the course of a child pornography investigation, FBI agents applied for a search warrant to search an apartment in Milwaukee, Wisconsin and all the computers found inside. On January 24, 2013, FBI agents executed the search warrant and seized sixteen electronic storage devices or hard drives. Order Denying Application to Compel Decryption, Docket ("Doc.") #3 at 1-2, *In re The Decryption of a Seized Data Storage System*, No. 13-M-449 (E.D. Wis. April 19, 2013). Of those sixteen devices, nine were encrypted. *Id.* at 2. After the FBI spent was unable to break the encryption, the government filed a request under the All Writs Act, 28 U.S.C. § 1651, asking the Court to order the apartment's owner, Mr. Feldman, to provide the decrypted contents of the devices to the government. *Id.* at 1-2; *see also* Application and Affidavit for Search Warrant as to Decryption of a Seized Data System, Doc. #1.

Magistrate Judge Callahan denied the request on April 19, 2013. Order Denying Application, Doc. #3 at 9. First he acknowledged that the act of producing the decrypted contents of the computer triggered Fifth Amendment scrutiny because it would put Mr. Feldman under risk of being compelled to provide incriminating testimony. *Id.* at 3. He rejected the government's argument that the existence of the evidence was non-testimonial as a "foregone

conclusion" because ultimately, the government had failed to prove with "reasonable particularity" that he had "personal access to and control over the encrypted devices." *Id.* at 9. Since forcing Mr. Feldman to decrypt the devices would thus give the government information it did not otherwise know, compelled decryption would violate the Fifth Amendment privilege against compelled incriminating testimony. *Id.*

After the Court denied the request, the government continued working to decrypt the devices. Request for Reconsideration, Doc. #5 at 2. Ultimately, it was able to decrypt one device not mentioned in the original affidavit and discovered pictures and other personal papers connected to Mr. Feldman as well as child pornography. *Id.* The government asked Judge Callahan to reconsider his earlier decision, and on May 21, 2013, the Court ordered Mr. Feldman to assist federal agents in decrypting the nine remaining hard drives. *See id*. Judge Callahan changed his mind because he felt that the discovery of Mr. Feldman's personal files on one storage device meant that the government had now shown it was a "foregone conclusion" that Mr. Feldman had access and control over *all* the encrypted devices. Order Granting Ex Parte Request for Reconsideration, Doc. #6 at 3.

On June 4, 2013, this Court granted Mr. Feldman's emergency motion to stay Judge Callahan's order pending review by this Court. Order Granting Motion to Stay Order, *In re Decryption*, Doc. #9.

ARGUMENT

A. Encryption is an Important and Routine Method of Safeguarding Electronic Data.

In an increasingly digitized world, encryption is an integral security feature to protect data. Encryption uses computer code to change plain, readable information into unreadable random letters, numbers and symbols. Encryption safeguards sensitive information by only

allowing this unreadable information – effectively gibberish – to be converted or deciphered into readable language through a specific code, commonly known as an "encryption key."[1]

What was once considered security for the highly technical is now an established part of modern technology. Apple's operating system, OS X, includes "File Vault," a program that allows users to encrypt the files in their home folders.[2] Microsoft's Windows operating system has included Bitlocker Drive encryption since 2008.[3] And information stored on-line, such as credit card or social security numbers are typically stored in an encrypted form as a means of safeguarding them from data theft.[4]

---

[1] *See generally* Wikipedia, *Encryption*, https://en.wikipedia.org/wiki/Encryption (last visited July 19, 2013).

[2] Apple explains "FileVault 2 uses full disk, XTS-AES 128 encryption to help keep your data secure. With FileVault 2 you can encrypt the contents of your entire drive." *OS X: About FileVault 2*, http://support.apple.com/kb/ht4790 (last visited July 23, 2013).

[3] As Microsoft notes on its website, "[h]ow can you help protect your data from loss, theft, or hackers? The answer: BitLocker. Improved for Windows 7 and available in the Ultimate and Enterprise editions, BitLocker helps keep everything from documents to passwords safer by encrypting the entire drive that Windows and your data reside on. Once BitLocker is turned on, any file you save on that drive is encrypted automatically." *BitLocker Drive Encryption*, http://windows.microsoft.com/en-us/windows7/products/features/bitlocker (last visited July 23, 2013).

[4] For example, Wells Fargo explains, "[f]rom the moment account information leaves your computer to the time it enters Wells Fargo's system, all online access and Bill Pay sessions are encrypted. Wells Fargo employs some of the strongest forms of encryption commercially available for use on the Web today. During any transaction, our 128-bit encryption turns your information into a coded sequence with billions of possible variations, making it nearly impossible for unwanted intruders to decipher." Wells Fargo, *How We Protect You*, https://www.wellsfargo.com/privacy-security/online/protect/ (last visited July 23, 2013). Bank of America does the same. *See* Bank of America, *Online Banking Security*, https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/online-banking-security.go (last visited July 23, 2013) ("Bank of America uses encryption technology, such as Secure Socket Layer (SSL), on its website to transmit information between you and the bank. This protects data . . . [by] . . . scrambl[ing] transferred data so that it cannot be read by unauthorized parties").

When the growing threat of unwarranted computer intrusions is coupled with the rise in the number of portable electronic devices being carried by Americans today – and the corresponding risk of loss or theft of those devices – it is clear that encryption is a crucial mechanism to safeguard both business and personal data in an increasingly digitized landscape. A number of Wisconsin state and local government agencies encrypt email correspondence in order to protect privacy. Barron County, for example, uses encrypted emails for employees needing to "exchange sensitive or private information such as Protected Health Information (PHI), Social Security numbers, medical record numbers, birth dates, account numbers."[5] The same is true of the Wisconsin Departments of Health Services,[6] Revenue[7] and Workforce Development.[8] In short, encryption is not a means to hide criminal behavior but a routine part of modern electronic life, no different than locking the door to your car or front door.

B. The Fifth Amendment Protects the Act of Compelled Decryption.

The Fifth Amendment to 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. This privilege against "self incrimination," prohibits "the use of physical or moral compulsion to extort communications" from an individual. *Holt v. United States*, 218 U.S. 245, 253 (1910).

To be protected by the Fifth Amendment, a person must show three things: (1) compulsion; (2) incrimination; and (3) a testimonial communication or act. *In re Grand Jury*

---

[5] *See Secure Email*, http://www.barroncountywi.gov/ (click on "Contacts" in the sidebar, then click on "Send us a Secure Email") (last visited July 23, 2013).

[6] *See* Wisconsin Department of Health Services, *Email Encryption*, http://www.dhs.wisconsin.gov/rl_dsl/publications/10-031.htm (last visited July 23, 2013).

[7] *See* Wisconsin Department of Revenue, *Common Questions: Secure Encrypted Email*, available at http://www.revenue.wi.gov/contact/SecureEncryptedEmailCommonQuestions.pdf (last visited July 23, 2013).

[8] *See* Wisconsin Department of Workforce Development, *Encrypted Email*, http://dwd.wisconsin.gov/asdhelp/encryptedemail.htm (last visited July 23, 2013).

Subpoena Duces Tecum Dated March 25, 2011 ("*In re Grand Jury Subpoena*"), 670 F.3d 1335, 1341 (11th Cir. 2012) (citing *United States v. Ghidoni*, 732 F.2d 814, 816 (11th Cir. 1984) and *United States v. Authement*, 607 F.2d 1129, 1131 (5th Cir. 1979) (per curiam)). A statement is incriminating if the answer either supports a conviction in a federal criminal case, or provides a "link in the chain of evidence" to lead to incriminating evidence, even if the statement itself is not inculpatory. *Hoffman v. United States*, 341 U.S. 479, 486 (1951), *see also United States v. Hubbell*, 530 U.S. 27, 38 (2000), *United States v. Doe*, 487 U.S. 201, 208-09 n.6 (1988); *Kastigar v. United States*, 406 U.S. 441, 444-45 (1972).

The term "testimony" refers not only to the act of speaking words from a person's mouth, but also to the act of producing documents. *Hubbell*, 530 U.S. at 36. In essence, the Fifth Amendment is implicated anytime a person must make use of the "contents of his own mind" to communicate a statement of fact. *Curcio v. United States*, 354 U.S. 118, 128 (1957). For example, the act of producing documents could be considered "testimony" if by producing the documents, the witness would be admitting that documents existed, were authentic, and in his possession or control. *Fisher v. United States*, 425 U.S. 391, 410 (1976).

There are two ways an act of production can be deemed non-testimonial. First, if the government compels a person to do a mere physical act that does not force an individual to make use of the contents of his mind, that act is non-testimonial. *Hubbell*, 530 U.S. at 43. Second, if the government can show with "reasonable particularity" that at the time it sought to compel production it already knew of the existence of the materials it was seeking, the Fifth Amendment is not implicated. *In re Grand Jury Subpoena*, 670 F.3d at 1346. In other words, since turning over the information – emptying the contents of one's mind – would not reveal anything to the government that it did not already know, the testimony is simply a "foregone conclusion."

Fisher, 425 U.S. at 411. If a court has done this analysis and determined that the government is attempting to compel incriminating testimony, the Fifth Amendment's privilege applies.

1. Decryption Is Not A Mere Physical Act But Reveals the Contents of Someone's Mind.

The Fifth Amendment is implicated anytime the government seeks to compel someone to decrypt computer files. As the Eleventh Circuit noted in *In re Grand Jury Subpoena*, the act of decrypting computer files reveals the contents of someone's mind. *In re Grand Jury Subpoena,* 670 F.3d at 1346. There, a grand jury subpoena was issued to John Doe, requiring him to produce the unencrypted contents of hard drives thought to contain child pornography. *Id.* at 1339. Doe objected that compliance would violate his Fifth Amendment right against self-incrimination because by decrypting the computer, the government would be compelling him to testify. *Id*. In essence, he would be testifying that he, instead of someone else, placed the contents on the hard drive, encrypted the contents and could retrieve and examine them as he wished. *Id.* Federal prosecutors offered Doe immunity for the act of decrypting the computer, but wanted to reserve the right to use any evidence it found on the computer against Doe. *Id.* The district court found that compelling Doe to produce the unencrypted contents of the hard drives would not constitute the derivative use of compelled testimony because Doe's act of decryption and production was not "testimony." *Id.* at 1341. It held Doe in contempt of court for refusing to decrypt the drives. *Id.* at 1340.

The Eleventh Circuit reversed the contempt ruling, holding that decryption was not merely a physical act, like providing officers with a key, but rather it would force someone to use the contents of their mind, similar to providing officers the combination to a safe. *Id.* at 1346 (citing *Hubbell*, 530 U.S. at 43). Decrypting a computer was the equivalent of testifying about the knowledge and existence of incriminating files, as well as a person's possession, control and

access to the encrypted drives and the ability to decrypt. *In re Grand Jury Subpoena,* 670 F.3d at 1346. The court noted, if "the decryption of the hard drives would not constitute testimony, one must ask, 'Why did the Government seek, and the district court grant, immunity?"' *Id.* at 1341 n. 13. The "obvious" answer was that "decryption would be testimonial." *Id.*

Other courts have essentially reached the same conclusion. In both *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012) and *In re Grand Jury Subpoena to Sebastien Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) the courts ultimately ordered the suspects there to decrypt devices but not because they found decryption was a mere physical act. Instead, of the two ways an act could be non-testimonial – either as a mere physical act or under the "foregone conclusion" doctrine – decryption was ordered in both cases under the "foregone conclusion" doctrine. *See Fricosu*, 841 F. Supp. 2d at 1237; *Boucher*, 2009 WL 424718 at *3. But the "foregone conclusion" doctrine does not mean that the act does not reveal the contents of someone's mind. Instead, because turning over the information would not reveal anything the government did not already know, "no constitutional rights are touched" since the government is not relying on the "truth telling" of the defendant, and therefore "the question is not of testimony but of surrender." *Fisher*, 425 U.S. at 411 (quoting *In re Harris*, 221 U.S. 274, 279 (1911) (quotations omitted)). In other words, a finding that the "foregone conclusion" applies does not mean that the testimony is merely a physical act, unprotected by the Fifth Amendment. *See also United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (compelled disclosure of encryption password was not mere physical act but required defendant to "divulge through his mental processes his password").

Since the act of decryption is not a mere physical act like turning over a key but reveals the contents of someone's mind, the Fifth Amendment protects a suspect from being compelled

to decrypt unless the government can carry its burden under the "foregone conclusion" doctrine to defeat the privilege.

2. The Government Has Failed To Show Mr. Feldman's Access and Control of the Devices is a "Foregone Conclusion."

Under the "foregone conclusion" doctrine, the Fifth Amendment is not implicated if the government can prove it is not asking a suspect to reveal something the government does not already know. *See Fisher*, 425 U.S. at 410-11. The court below believed the Seventh Circuit would adopt the approach of other circuits addressing the doctrine and ruled that in order for the government to call upon the doctrine, it had to "establish its knowledge of the existence, possession, and authenticity of the subpoenaed documents with 'reasonable particularity' before the 'foregone conclusion' doctrine applies." Order Denying Application to Compel Decryption, Doc. #3 at 5, 7 (quoting *United States v. Ponds*, 454 F.3d 313, 320-21 (D.C. Cir. 2006); *In re Grand Jury Subpoena, Dated April 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004); *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992,* 1 F.3d 87, 93 (2d Cir. 1993)).

When it comes to the issue of decryption, the Eleventh Circuit has provided crucial guidance about the showing the government must make to carry its burden under the doctrine:

> if the Government is unaware of a particular file name, it still must show with some reasonable particularity that it seeks a certain file and is aware, *based on other information*, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic.

In re Grand Jury Subpoena, 670 F.3d at 1349 n. 28 (citing *United States v. Norwood*, 420 F.3d 888, 895–96 (8th Cir. 2005)) (emphasis added). "[A]lthough the Government need not know the name of a particular file or account, it still must be able to establish that a file or account, whatever its label, does in fact exist." *In re Grand Jury Subpoena*, 670 F.3d at 1349. It was knowledge "based on other information" that distinguished Doe's case from *Fricosu* and

Boucher where the Court found the foregone conclusion doctrine warranted compelled decryption.

In *Fricosu,* FBI agents executed a search warrant at Fricosu's home and seized a number of computers. *Fricosu*, 841 F. Supp. 2d at 1234. One of the laptops found in Fricosu's bedroom was encrypted, and identified itself as "RS.WORKGROUP.Ramona" on the whole disk encryption screen. *Id.* At the time of the search, Fricosu's ex-husband and co-defendant was incarcerated on unrelated charges. *Id.* at 1235. The day after the search, Fricosu's husband spoke to her over the telephone from prison. *Id*. The telephone call was recorded and included Fricosu telling her ex-husband "they will have to ask for my help," "can they get past what they need to get past to get to it," 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*. The FBI was unable to decrypt the laptop and sought to compel Fricosu to provide the unencrypted contents of the computer. The court found the fact the computer was identified as "RS.WORKGROUP.Ramona," as well as the comments Fricosu made on the telephone to her ex-husband was additional information that allowed the government to satisfy its burden under the foregone conclusion doctrine. *Id.* at 1237.

In *Boucher*, the suspect approached the United States border from Canada near Vermont. Border agents saw a laptop computer in the back seat of the car, which Boucher admitted was his. An agent decided to inspect the computer and found approximately 40,000 photographs on it. *Boucher*, 2009 WL 424718 at *1. The images included both adult and child pornography. *Id.* at *2. After Boucher waived his *Miranda* rights, he agreed to speak to the agents and opened files on the "Z drive" on the computers at the officers' request. After viewing more images and videos of child pornography in the "Z drive," the agents arrested Boucher and confiscated his

laptop. Later, agents obtained a search warrant. While creating a mirror image of the contents of the laptop, they discovered that the "Z drive" from which Boucher had previously opened files for the officers was encrypted. As a result, the officers were unable to take a mirror copy of the contents of the "Z drive." The grand jury subpoenaed Boucher to provide the unencrypted contents of the computer instead. *Id.* at *2. The magistrate initially quashed the subpoena but the district court reversed, finding the "foregone conclusion" doctrine rendered the act of producing the decrypted contents of the computer non-testimonial. *Id.* at *3. The government knew of the existence and location of the files since Boucher had showed them to the officers personally. Nor did the order compel Boucher to authenticate the contents of the computer, since he had already done so by admitting the laptop was his and showing officers files and folders on it. *Id.* at *4. Thus, providing access again did "little or nothing to the sum total of the Government's information." *Id.* at *3 (quoting *Fisher*, 425 U.S. at 41) (quotations omitted).

In contrast to *Fricosu* and *Boucher*, the Eleventh Circuit found the government failed to show Doe's testimony was a "foregone conclusion," noting that there was nothing in the record that revealed the government knew whether files existed on the drive, where they were located, or that Doe was capable of decrypting them. *In re Grand Jury Subpoena*, 670 F.3d at 1346-47. It rejected the government's suggestion that the fact the drives were encrypted meant Doe was trying to hide something, noting "[j]ust as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all." *Id.* at 1347. In the absence of "other information" like Fricosu's discussion of the contents of the computer with her ex-husband on a recorded phone call, or Boucher displaying the incriminating evidence directly to officers and authenticating the computer itself,

the foregone conclusion doctrine did not apply and the Fifth Amendment was implicated. *Id.* at 1348, 1349 n. 27.

This case is more like the Eleventh Circuit's decision in *In re Grand Jury Subpoena* than either *Fricosu* or *Boucher*. In its first order, the magistrate noted that forensic examination of an unencrypted Dell computer showed the "I" drive on the Dell computer could correspond to one of two drives and that the "F" and "G" drives on the computer could correspond to any of the other connected devices. Order Denying Application to Compel Decryption, Doc. #3 No. 3 at 2-3. The court also noted that the devices were found in Mr. Feldman's residence and that the unencrypted Dell computer had Mr. Feldman's name as its only login. *Id.* As the magistrate correctly held, these facts were insufficient to demonstrate access and control over the storage devices because "unlike in *Boucher* and *Fricosu*, here, Feldman has not admitted access and control." *Id.* at 9. In *Boucher*, the suspect literally exercised dominion and control over the devices in front of federal agents. *Boucher*, 2009 WL 424718 at *2. And in *Fricosu*, the suspect "essentially admitted every testimonial communication that may have been implicit in the production of the unencrypted contents" during the recorded conversation with her ex-husband. *In re Grand Jury Subpoena*, 670 F.3d at 1349 n. 27 (citing *Fricosu*, 841 F. Supp. 2d at 1235). In contrast, here the government is armed with no additional facts or admission by Mr. Feldman that he had access and control over these devices. That means the government failed to carry its burden of showing the facts to be revealed by forced decryption – namely Feldman's access and control over the devices – was a foregone conclusion.

The court changed its mind, however, because of the government's ability to decrypt a portion of one drive. Order Granting Ex Parte Request for Reconsideration, Doc. #6 at 3. But that fact alone is not enough to permit the government to carry its burden. At best, the

government has proven Mr. Feldman had "access and control" over the one device it was able to decrypt.[9] But the government has pointed to nothing to demonstrate with "reasonable certainty" that Mr. Feldman had access and control to the *remaining devices*. Nor is there any indication that the government has proven with reasonable certainty that Mr. Feldman had exclusive access to the Dell computer where these devices purportedly were connected to at some point.[10] Storage devices are by their nature portable to enable easy sharing and collaboration and could be accessed or used by other people. Without something more – either a clear act or an admission of access and control by Mr. Feldman as was the case in *Boucher* or *Fricosu* – the government cannot carry its burden under the foregone conclusion doctrine and the Fifth Amendment prohibits any attempt to force Mr. Feldman to decrypt the contents of the storage devices.

C. This Court Must Grant Mr. Feldman Immunity From Government Use of Any Evidence Found on the Storage Devices to Preserve the Fifth Amendment Privilege.

Since the Fifth Amendment privilege applies, this Court is faced with two options: it can either deny the writ outright or it can compel Mr. Feldman to testify by offering him immunity. Immunity has long been a "rational accommodation" between the Fifth Amendment privilege and the government's ability to compel individuals to testify. *Kastigar*, 406 U.S. at 446. The

---

[9] Even with respect to the one drive the FBI was able to decrypt, the existence of Mr. Feldman's personal files in some of the folders is only enough to connect him to the specific folders those files were found rather than the entire drive.

[10] The Dell computer containing Mr. Feldman's name on the login screen was unencrypted, an important fact that distinguishes this case from *Fricosu*. The computer in *Fricosu* was encrypted and the encryption screen had Fricosu's name on it, meaning there was stronger "additional information" suggesting that Fricosu had accessed and controlled the encrypted mechanism on the computer itself. *See Fricosu*, 841 F. Supp. 2d at 1234. While the lower court found that the government proved Mr. Feldman was "capable of using encryption," that alone is not enough to show he *actually* encrypted the devices. Order Granting Ex Parte Request for Reconsideration, Doc. #6 at 3.

federal immunity statute, 18 U.S.C. § 6002, states that if an order to testify has been given to a witness,

> …the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case…

18 U.S.C. § 6002. In *Kastigar v. United States*, 406 U.S. 441 (1972), the Supreme Court explained that historically, any immunity granted under a statute, including 18 U.S.C. § 6002, must be "coextensive" with the Fifth Amendment privilege. *Kastigar*, 406 U.S. at 449 (citing *Murphy v. Waterfront Comm'n*, 378 U.S. 52, 54, 78, (1964); *Counselman v. Hitchcock*, 142 U.S. 547, 585 (1892)). That means the immunity must prohibit the government "from the use of compelled testimony, as well as evidence derived directly and indirectly therefrom." *Kastigar*, 406 U.S. at 453. These two forms of immunity have been described as "use" and "derivative use" immunity. When it comes to how immunity applies to the act of compelled decryption, the Eleventh Circuit's decision in *In re Grand Jury Subpoena* is directly on point.

The court there ruled the use immunity offered Doe – a promise not to watch Doe enter an encryption password or use the password itself against him – was insufficient and that derivative use immunity – a prohibition from using any evidence obtained against Doe – was necessary. *In re Grand Jury Subpoena*, 670 F.3d at 1350-52. Noting the critical issue was "what conduct was actually immunized and what use would the Government make of the evidence derived from such conduct in a future prosecution," it ruled that 18 U.S.C. § 6002 "clearly immunizes both the use of the testimony itself and any information derived from the testimony." *Id.* at 1349-50, 1350 n. 31. That meant no evidence found on the drives could be used against Doe if he were to decrypt the drives, since any files found would be "directly or indirectly

derived from" the compelled testimony. *Id.* at 1352 n. 33 (quoting *Kastigar*, 406 U.S. at 453 (quotations omitted)).

The exact same situation is present here. Because immunity must be coextensive with the privilege, if Mr. Feldman is ordered to decrypt the contents of the storage devices, the government must be prohibited from making use of *any* data it finds on the devices in a criminal case against Mr. Feldman. The Supreme Court has already rejected a "manna from heaven" theory, or the idea that there is no constitutional problem if the government merely refrains from using the fact the suspect turned the information over to it to use, but then makes "substantial use" of the information to indict the suspect. *Hubbell*, 530 U.S. at 33, 42–43.

Yet that is precisely what the government is trying to do here. The government cannot simply immunize Mr. Feldman from the mere act of production and then use the contents of that production because that would permit the derivative use of the evidence. *See In re Grand Jury Subpoena*, 670 F.3d at 1352. Thus, the only way to protect Mr. Feldman's Fifth Amendment privilege against compelled testimony is to grant him immunity coextensive with his privilege by prohibiting the government from using any of the evidence it derives from decryption against Mr. Feldman in a later criminal case if one is brought.

CONCLUSION

The Fifth Amendment privilege is an important bulwark between the government and common citizens. While the government should absolutely have the ability to investigate and prosecute serious crimes, it cannot force a suspect to decrypt electronic devices when doing so provides the government with testimony it would not otherwise have: that the suspect has dominion and control over the device, and thus the incriminating contents inside. This Court

should deny the government's requested writ and find that the Fifth Amendment protects Mr. Feldman from decrypting the storage devices.

Dated this 23rd day of July, 2013 at San Francisco, California.

Respectfully submitted,

/s/ Hanni M. Fakhoury

Hanni M. Fakhoury
CA Bar No. 252629
Counsel for Amicus Curiae
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
hanni@eff.org