UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

v. Case No. 13-MJ-00449-RTR

DECRYPTION OF A SEIZED
DATA STORAGE SYSTEM,

Defendant.

INTERESTED PARTY JEFFREY FELDMAN'S BRIEF IN OPPOSITION TO ALL GOVERNMENT EFFORTS TO FORCE HIM TO ATTEMPT TO DECRYPT COMPUTER DRIVES SEIZED FROM HIS RESIDENCE

INTRODUCTION

The Government is attempting to misuse the All Writs Act to circumvent the Fifth Amendment rights afforded to Mr. Feldman in place of seeking a Grand Jury indictment, thereby forcing a non-indicted defendant to choose between his Fifth Amendment right against attempting to decrypt and the possibility of indefinite incarceration. This Court must reject and condemn this coercive effort to circumvent constitutional protections and well-established laws and procedures.

The government in its pre-indictment filings under the All Writs Act claims to have found child pornography in unspecified portions of what has been described as a part of the Feldman storage system. Ordinarily, the next step in this process is an indictment, followed by the disclosure of the computer forensic reports usually from EnCase, FTK or a similar forensic program utilized by the Government analysts that duplicates, partitions, and searches for images (jpg. or mpg.). The next step in the legal process is often a challenge to the application for the warrant where the indicted person

could challenge whether there was probable cause and/or whether the application contained reckless omissions and or misstatements.[1] Mr. Feldman cannot be compelled to do an act that produces evidence that may save the Government's search under doctrines such as good faith or inevitable discovery.

I. THE ALL WRITS ACT IS NOT THE PROPER VEHICLE FOR COMPELLING MR. FELDMAN TO ATTEMPT TO DECRYPT AS OTHER ALTERNATIVES EXIST AND THE GOVERNMENT HAS NOT PURSUED THEM.

The All Writs Act ("The Act") is not the proper vehicle for compelling Mr. Feldman to attempt decrypting the seized drives, because the Act is "an extraordinary remedy," only available for accomplishing certain purposes when no other vehicles exist to attain them. *See In re Montes*, 677 F.2d 415, 416 (5th Cir. 1982) ("[I]t is well settled that relief under the All-Writs Act is not available unless the applicant has shown that he has no other adequate remedy"), *citing In re: Chicago, R.I. & P. Ry.*, 255 U.S. 273 (1921); *Noble v. Eicher*, 143 F.2d 1001 (D.C.Cir.1944). "Under the All Writs Act, the form is less important than the substantive question [of] whether an extraordinary remedy is available." *In re Davis,* 730 F.2d 176, 181 (5th Cir.1984). To ensure the use of writs in only "extraordinary situations," the Supreme Court has established two prerequisites to the issuance of a writ: (1) that the petitioner have no other "adequate means to attain the [desired] relief," and (2) that the petitioner meet its burden of showing that its right to the writ is "clear and indisputable." *Kerr v. U.S. Dist. Court for Northern Dist. Of California,* 426 U.S. 394, 403 (1976).

[1]The government avers in the application for the warrant that it could not locate a single-source download for the pornography that was identified in the application as known images of child pornography. In the world of Peer to Peer (P2P) Networks, when a file is requested to be downloaded, it can be, and many times is downloaded from multiple sources (computers) in different locations and then reassembled at the client end. This is possible by identifying exactly the same file at different locations using the Sha1 values.

In this case, the government may not utilize the All Writs Act to force Mr. Feldman to attempt to decrypt the seized drives because other vehicles exist, remain available, and have not been not exhausted by the Government. The first viable alternative is convening a Grand Jury and calling Mr. Feldman as a witness, perhaps with a subpoena *duces tecum* for any passwords he may possess or have memorized. This would afford Mr. Feldman the usual Fifth Amendment protections given to any individual called as a witness who may incriminate themselves. Should Mr. Feldman invoke the Fifth Amendment in front of the Grand Jury, the government could then offer him immunity co-extensive [2] with the Fifth Amendment in order to attempt to have him decrypt the drives. If he refused to decrypt after being granted co-extensive immunity, then the government would be well within its rights to ask he be held in contempt, and this Court could then lawfully do so (assuming, of course, that the government can make an adequate showing that he in fact can decrypt the drives, which Mr. Feldman does not concede he can do).

The second viable alternative is for the government to subpoena information from the manufacturer to aid it in its decryption process. The government has made no showing that it has attempted to get help in its decryption efforts from the manufacturer, or to enlist the aid of outside experts who may have the needed expertise to decrypt the drives. The government offers no authorities, and Mr. Feldman asserts than none exist, supporting the Act's use for this purpose.

The Government in its initial filings avers that the issuance of the search warrant by the magistrate is meaningless if the Government cannot force decryption. Practically

[2] Meaning use and derivative-use immunity, not just act-of-production (of the passwords, if he in fact can produce them) immunity.

speaking, all hard drives sold in the last few years are encrypted by the manufacturer and thus this discussion belongs in Congress not in Court. Congress has been debating whether manufacturers' must provide a "back door" so that the government can get access should a particular situation require it. The government has seized what the warrant allowed it to seize. It is in the possession of all the seized items. Nothing supports the government's attempt to use the Act ostensibly to further the execution of a warrant, which had already been successfully executed prior to the government's request invoking the Act. The government in effect impermissibly employs the Act to extend the reach of the already-executed warrant, so as to seize the contents of Mr. Feldman's mind: his (assumed) knowledge of the passwords, knowledge of the existence of (assumed illegal) files, ability to access to such files, etc. Mr. Feldman respectfully asks this Court to heed the Supreme Court's admonishment and exercise its writ power here with caution. *See Kerr* at 402. Because the remedy is so extreme, this Court should invoke it only "in extraordinary situations." *See id*. Here the situation is not "extraordinary" because the government can proceed by other means and it has not made any showing or assertion it has attempted to do so.

II. THE FIFTH AMENDMENT AND ENCRYPTED DIGITAL DATA.

Generally speaking, for Fifth Amendment protections to apply, an individual must show (1) compulsion, (2) testimonial communication or act, and (3) incrimination. *See In re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011, U.S. v. John Doe*, 670 F. 3d 1335, 1341 (11th Cir. 2012); *see also* fn 15 (Fifth Amendment prohibits compelled production not just of directly-incriminating evidence itself, but also of anything constituting a "link in the chain" that leads to such incriminating evidence); *see also*

United States v. Hubbell, 530 U.S. 27, 38 (2000).

Several cases address the Fifth Amendment and compelled production of existing physical materials, and that law is well established. *See discussion infra*. But very few decisions address compelled decryption of digital data, and compelling decryption of digital data poses several new legal issues and challenges to the existing doctrine. The sole published federal court of appeals case on compelled decryption of digital data -- thus the most compelling source of persuasive authority for this Court to consider -- is *Doe*, *supra*.

In *Doe* the defendant, like Mr. Feldman, made no admissions of ownership, access, or possession of the seized computers or files, and the government lacked direct evidence of incriminating data on the drives in question. It subpoenaed the unencrypted contents of the seized hard drives. When Doe invoked the Fifth Amendment, the government offered Doe limited act-of-production immunity and sought to compel compliance with the subpoena. When such orders were issued, Doe refused to decrypt. When the Government sought a contempt order against Doe, Doe argued that the Fifth Amendment protected him from the government's derivative use of the act of decryption, a protected "testimonial" act outside of the granted immunity. Doe also stated he was unable to decrypt the drives. The court rejected Doe's arguments and ordered him in contempt. Doe appealed the ruling while incarcerated and eventually was released upon the Eleventh Circuit's decision.

The Eleventh Circuit held that the compelled act of decryption would be "testimonial" (as revealing the contents of the mind of the decrypting person), thus protected by the Fifth Amendment; and that limited act-of-production immunity

insufficiently accommodated the Amendment's protections. The Court in *Doe* held that: the government could not compel decryption, unless it offered immunity coextensive with Fifth Amendment protections. Asked whether compelled decryption would incriminate Doe, the court realistically determined that it would indeed give the government information it lacked, e.g. that data existed on the encrypted drives, that Doe had knowledge, access and possession of the drives, and that the data the government sought was authentic. This common-sense focus undergirded the holding that the Fifth Amendment protected Doe from self-incrimination by decryption, unless properly immunized.

As in *Doe*, a key issue in Mr. Feldman's case is the testimonial aspect of forcing Mr. Feldman to try to encrypt. *See Doe* at 1342. Most important, in both cases the act of compelled decryption would not merely convey to the government the decrypted *contents* of the drives (if such exist), but would provide the government with *otherwise lacking* direct evidence of the descriptor's access to and control of the potentially incriminating contents, his knowledge of the contents' existence and location, his ability to decrypt and access it, and arguably even his guilty conscience, of which encryption could be a sign. As in *Doe*, Mr. Feldman's own act of decryption would communicate multiple facts which could be used to convict Mr. Feldman -- facts which the government does not know from elsewhere and has no other direct ways of proving. Despite *Doe*, the government repeatedly argues as though the act of decryption were self-evidently not testimonial, but instead cognitively neutral, revealing nothing but the "decrypted contents" of the drives. *Doe* clearly holds otherwise, relying on the older "testimonial act" jurisprudence that the government now would ignore or forget.

Beyond *Doe*, two seminal cases supply the jurisprudence of "testimonial acts": *Fisher v. United States*, 425 U.S. 391 (1976) and *Hubbell* (recognizing that acts which implicitly communicate facts unknown to the government from other sources are privileged, testimonial and incriminating, thus protected under the Fifth Amendment). In light of this well-settled law, if the government is trying to compel an individual to use the "contents of his own mind" to explicitly or implicitly communicate any statement of fact that could incriminate him, then such use is "testimonial," activating Fifth Amendment protections. This is the case here, as argued above.

The Supreme Court has identified only two situations where an act of production is clearly not testimonial and therefore not covered by the Fifth Amendment, and neither exists here: first, when the government tries to compel the performance of some physical act (i.e. voice exemplar or handwriting sample). This scenario is clearly inapplicable to Mr. Feldman's case, where the government is attempting to force him to reveal or use the contents of his mind and not merely perform some physical act. Second, when the government can show with "reasonable particularity" that at the time it sought to compel the act of production of certain pre-existing materials or contents, it already knew such materials or contents existed, thereby making any testimonial aspect a "foregone conclusion."

The government here repeatedly invokes the "foregone conclusion" doctrine in its applications and motions. But the government has not shown with "reasonable particularity" that any of the seven decrypted drives it asks Mr. Feldman to attempt to decrypt contains any readable data at all, much less child pornography. The government only vaguely asserts that "files constituting child pornography" exist on the "the storage

system." The government does not say such files exist on any of the seven encrypted drives; even more fatal to the government's attempt to force Mr. Feldman to decrypt the drives is its failure to allege or offer any showing on whether the drives contain data at all and are not merely blank or wiped clean. It alleges no facts supporting Mr. Feldman's ability to decrypt any of the drives. It alleges no facts showing that Mr. Feldman was the only person with access to the drives or possession/control of them: although he lived at his address alone, others may have used his computer and drives over the years or they may have belonged to someone else. Also, the government has failed to show other parties, such as the manufacturer or any other expert, can access the data on the drives.

Doe, Fisher and *Hubbell* all strongly support that, by the act of decryption, Mr. Feldman would be "a witness against himself," i.e. would provide to the government (perhaps implicitly) novel information about his knowledge and possession of, and access to, potentially incriminating data in the drives. This Court should find that Mr. Feldman's act of decryption is protected by the Fifth Amendment and does not have to be done absent a grant of co-extensive immunity.

III. FRANKS ISSUES

The government's pleadings in this proceeding pose several concerns under *Franks v. Delaware,* 438 U.S. 154 (1978), where agents -- knowingly and with reckless disregard for the truth -- overstate or exaggerate facts, omit or gloss over potentially dispositive details, and paint a picture to suit their needs by manipulative insinuation and implication.

A. The term "storage system" is used misleadingly, making it sound like one integrated system, instead of multiple, individual and separate hard drives or "storage medium."

The government describes the seized computer and hard drives as a "storage system" and the affidavits assert that the drives are, or were, interconnected. Docket Entry 5-1, page 1, paragraph 2(b). However, nothing is offered to support this convenient assertion or definition. The government defines "storage medium" as any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here." Docket Entry 1-1, page 2, paragraph 8(a). Equating discrete, individual and separate "storage medium" with a vague and generic "storage system" recklessly disregards the truth when no facts are asserted to show that the media indeed function, or once functioned, so that data was "shared, copied and transferred" between these "interconnected" devices.

This reckless obfuscation, by specious inference and without support, allows the government to claim that if *one* drive contained Mr. Feldman's data and was accessible to him, and perhaps ("allegedly") at one time had child pornography "available for download," then any of the still-encrypted drives/media might do so. This ungrounded presumption remains unsupported by fact.

B. The phrase "intricate electronic folder structure comprised of approximately 6,712 folders and subfolders" with "approximately 707,307 files" is misleading.

The agents solemnly declare, in Docket Entry 5-1, page 1, paragraph 2(c), that the decrypted drives -- misleadingly here described as "part of a storage system," *see supra* -- contains an "intricate electronic folder structure comprised of approximately 6,712

folders and subfolders" with "approximately 707,307 files." This language suggests that the drive bears the stamp of Mr. Feldman's extensive misbehavior and advanced technical skill: the "intricacy" of the folder structure and the seemingly huge number of folders and files so suggest. They also suggest that a rich bounty of child pornography can be discovered upon decryption.

This is misleading obfuscation, made in reckless disregard of this truth: any and all computers with the Windows operating system, for example, "contains an intricate electronic folder structure" with thousands of folders and subfolders and hundreds of thousands of files. The very computer upon which this brief is being written has a folder on its hard drive titled "Windows," and contains over 33 gigabytes of data located in 143,464 files in 25,537 folders. There mere number of files and structure of folders does not indicate one way or the other whether a given computer or hard drive contains contraband, or innocuous computer files that any modern computer needs in order to run.

C. The phrase "numerous files which constitute child pornography" is not demonstrated by the government in its filings.

This language, found in the most recent affidavit, Docket Entry 5-1, page 1, paragraph 2(c), is intentionally misleading: the government nowhere asserts that any files on the seized drives contain "images" or "pictures." "Files" could mean file names, deleted files, or file fragments. "Constitute" camouflages the government's mental short cut, meaning: "files which the government believes could be related child pornography, because of some possible connection with child pornography," such as a file name.[3]

[3]A *Franks* hearing was held in *United States v. Matthew Anderson*, 08-CR-261-RTR, wherein Magistrate Goodstein found that "Regardless of this precise nature of Hoell's belief, the determination that had to be made when Hoell requested approval to search Anderson's hard drive was whether there was probable cause to believe that Anderson possessed child

This misleading language recklessly disregards the fact that the government only *suspects* that child pornography was or may be on any encrypted drives. Nothing in the government's filings shows directly that child pornography was or is on any of the drives: no admissions, no witness observations, and no record of single-source downloading. The government does not in any way identify any of the files "constituting" child pornography on any Feldman drive: no logs, no hash tags on the drives sought for which compelled decryption is sought

D. The phrase that the encrypted drives "contain data" is misleading and not substantiated in any way.

Docket Entry 1-1, page 6, paragraph 23 states: "A forensic analysis of the nine encrypted drives . . . shows that they contain data."

This assertion displays a reckless disregard for the truth because, while it appears to be conveying information, it in fact does not. The "contains data" language only insinuates a slew of options but provides no concrete information and no supportive factual detail to figure out what "contains data" means: is it discernible and readable data? Or scrambled digits? Or blank space, which in the digital universe also manifests as data? Or is it simply the information the manufacturer puts on the drive to make its use possible as a storage vehicle?

This sort of misleadingly and obfuscating drafting -- which can hardly be inadvertent -- is *Franks*-hearing-worthy because by indulging in it the government

---

pornography on a portable hard drive found in his backpack. For this determination, the fact that the files had been deleted was highly relevant. Although it certainly is not necessary for an affiant to include every detail of an investigation in an affidavit submitted in support of a search warrant, on a crucial issue such as probable cause to believe that the suspect still had access to the relevant contraband, it is incumbent upon the affiant to include this information so as to permit the reviewing judicial officer to determine its significance".

manages to create a fuzzy false picture which serves its ends, but which does not reflect the investigative facts in its possession.

E. Describing Mr. Feldman as a "competent software developer" who "could have learned" advanced encryption insinuates he has ominous expertise and only a person having such traits could encrypt data.

Describing Mr. Feldman as a "competent software developer" who "could have learned" advanced encryption, *see* Document 1-1 at pages 9-10, misleads by insinuating that he has ominous expertise which he nefariously abused -- neither of which the government can support with facts. This language misleads the reader into perceiving Mr. Feldman as exceptionally skilled, dangerously smart, and on the verge of escaping prosecution.

It recklessly disregards, or knowingly omits to state, the evident truth that today anyone can learn to encrypt and decrypt relatively quickly and easily, and his or her encryption efforts can all be extremely hard to break. If this is the case then all of the companies listed as an exhibit to Docket Entry 7, previously submitted by Mr. Feldman, are engaging in the crimes of mail and wire fraud. Docket Entry 7-1 at pages 12-18.

F. Hardware encryption can be done automatically by the hard drive and is not necessarily done by the user.

And even more important and conveniently over-looked in the Government's filings is that today's computer hardware comes with its own default hardware-level encryption mechanisms pre-enabled, so encryption happens often without the user's involvement. For example, Western Digital, a key manufacturer of hard drives, warned its customers as early as 2011 that its new drives come with standard 256-Bit encryption, which is activated and occurs without any act on the user's part. This feature sometimes

causes customers/users lose access to their own data -- when their drives perform encryption which the users cannot break. *See* attached "Warning to Customers with new WD hard drives." (See Exhibit 1). This warning standing alone constitutes a material omission and should cause any Court addressing this issue a reason to pause.

Mr. Feldman submits that the above constitutes a "preliminary showing" of the government's attempt, via this proceeding, to obtain evidence by intentionally and/or recklessly including material false information in its affidavits to its Application, and Request for Reconsideration. Mr. Feldman thus requests a hearing pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978); *see also United States v. McDuffy,* 636 F.3d 361, 363 (7th Cir.2011). Mr. Feldman has previously asked this Court to order disclosure of the forensic attempts made by the government to access data contained on the encrypted drives. Without that forensic data, Mr. Feldman is denied effective assistance of counsel and unable to fully present the *Franks* issues that taint the affidavits in this case.

IV. NEED FOR A NEW ANALYTIC FRAMEWORK

The existing Fifth Amendment jurisprudence concerns the compelled production of pre-existing, intentionally created physical documents or items, *e.g.* as when documents are pulled from a safe or filing cabinet by unlocking each container. Decryption of digital data, in any medium, is essentially different and calls for new developments in Fifth Amendment analysis. *See* McGregor article at 584-85, 595 (considering the distinct "nature of encryption" as a ground for a "different analysis" than is available in law) *see also* McGregor at 602-604 (proposing a shredding analogy to describe how encryption alters data and how decryption requires re-constituting or re-constructing it) and 609 (noting that the unique nature of encrypted data warrants a

distinct analysis than other secured documents; noting that decryption requires "reconstituting" of encrypted, thus altered-beyond-any-recognition, data).

Decryption has been likened to a process of re-assembling or re-creating data, and data or documents that are made or created under compulsion pose very different Fifth Amendment concerns than data or documents that are merely turned over or revealed. *See Hubbell* at 35-36 and at fn 18. The Supreme Court has noted the distinction of assembling or creating data versus merely surrendering it by comparing the difference in having to disclose the combination to a wall safe versus having to turn over the key to a strongbox. *See Hubbell* at 43; s*ee also Fisher* at 411 (the "question is not of testimony but surrender"). The former forces the individual to use the contents of his or her mind to possibly incriminate them, where the latter merely forces them to perform a physical act. Once a document or a picture is encrypted, the new file becomes transformed into a meaningless number of characters; the forced act of decryption compels not only the surrender of such documents, but compels the person to re-make or recreate them.

A novel legal issue emerges from the technological fact that decryption by necessity involves producing anew what does not exist in the encrypted state (e.g. text files, comprehensible data, recognizable images): does compelled decryption constitute compelled production of self-incriminating evidence, which is clearly prohibited by the Fifth Amendment?

Mr. Feldman asks this Court to refine and develop the dated analytical framework by resolving this novel legal issue consistent with the Fifth Amendment protections afforded by *Doe* so that that compelled decryption *would not require him to produce what currently does not exist*, and might incriminate him if he is compelled to do so.

CONCLUSION

The "foregone conclusion" doctrine and All Writs Act are today the government's subtler and more far-reaching means of avoiding the protection of the Fifth Amendment. They illustrate the discovery and invention which allow the government, by means far more effective than stretching upon the rack, to obtain encrypted data. Among the subtler and more far-reaching means are also the government's artfully-worded warrant applications and affidavits, falsely suggesting that compelled decryption will yield only "foregone conclusions," as in Mr. Feldman's case; and its artfully-worded subpoenas falsely suggesting that only material objects or document contents are being extracted, not any contents of the mind. Mr. Feldman's act of compelled decryption would reveal the contents of his mind, providing the government information it now does not have nor can prove independently, and would thus be "testimonial" and privileged under the Fifth Amendment. Compelled decryption would require Mr. Feldman to produce what does not exist in an encrypted state, but what could incriminate him if produced, and thus would violate the Fifth Amendment. Compelled decryption may aid the government in saving an application that lacks probable cause. The government's pursuit of and execution of a search warrant in this case does not automatically require compelled decryption of any seized and encrypted digital data.

This coercive threat is real: Doe spent several months in custody before succeeding in the Eleventh Circuit. As has been previously stated, Mr. Feldman asserted his Fifth Amendment rights during the execution of the search warrant. Hired counsel the following day, without compulsion, provided information as to Mr. Feldman's whereabouts and indicated Mr. Feldman would promptly self-surrender should a warrant for his arrest issue. Mr. Feldman respectfully asks this Court to re-affirm the Fifth

Amendment and its protections, thereby to effectuate the no-coerced-convictions goal of the Constitution's framers, in the interest of liberty.

REQUESTED RELIEF

Mr. Feldman asks this Court to quash the Government's Application Under the All Writs Act, Docket Entry 1, because it impermissibly attempts to use the All Writs Act to avoid the still-available path of seeking Grand Jury indictment, even if that would require granting Fifth Amendment-coextensive immunity; and because it brutally coerces Mr. Feldman to self-incriminate, by threatening incarceration for refusal to follow the requested order, if granted.

Mr. Feldman asks this Court that if it does not deny the Governments request instanter, that the Court schedule a *Franks* hearing that allows for sufficient time to obtain experts to review the forensic testing to review the analysis that the Government purports to have already done on the encrypted drives pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978). At the hearing Mr. Feldman will examine the government's agents regarding the forensic reports and the agents' assertions in the affidavits, Application, etc., to support his *Franks* arguments. Mr. Feldman has made the "preliminary showing" that the government via this proceeding seeks to obtain evidence by intentionally or recklessly including material false information in its affidavits, Application, and motion. *Id.* at 155 – 156; *United States v. McDuffy,* 636 F.3d 361, 363 (7th Cir.2011).[4]

[4] Based on this Court's briefing order, this Brief addresses only the Government's Application Under the All Writs Act, Docket Entry 1, and subsequent Ex Parte Request for Reconsideration, Docket Entry 5. This Brief does not respond to the government's Motion to Require Jeffrey Feldman to Provide the Court with the Decrypted Contents of his Encrypted Digital media, *Ex*

Dated at Milwaukee, Wisconsin, this 16th day of July, 2013.

Respectfully Submitted,

s/Robin Shellow_____
Robin Shellow, #1006052
Urszula Tempska, #1041496
324 W. Vine Street
Milwaukee, WI 53212
(414) 263-4488
tsg@theshellowgroup.com

Christopher Donovan
State Bar No. 1055112
Pruhs & Donovan, S.C.
757 N. Broadway #401
Milwaukee, WI 53202

Attorneys for Jeffrey Feldman,
Interested Party

Parte and Under Seal, Docket Entry 10. Mr. Feldman responded to this last motion, Docket Entry 12, but would welcome further briefing on the issue raised in the government's motion should this Court so desire.