UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN

In the Matter of the Decryption of a Seized Data Storage System	)	Case Number: 13-M-~~421~~ 449

Application Under the All Writs Act Requiring Jeffrey Feldman to Assist in the Execution of Previously-Issued Search Warrant

I. Introduction

The United States of America, by and through James M. Santelle, United States Attorney, and Karine Moreno-Taxman, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Jeffrey Feldman to assist in the execution of a federal search warrant by providing federal law enforcement agents a decrypted version of the contents of his encrypted data storage system (hereinafter "Storage System"), previously seized and authorized for search under a federal search warrant, 13-M-421 ("Search Warrant").

II. Background

The Federal Bureau of Investigation ("FBI") currently has in its possession the Storage System, which was seized pursuant to the Search Warrant. (Banner Aff. ¶ 12). Initial inspection of the Storage System revealed that significant portions of it are encrypted. (Banner Aff. ¶ 15). Because parts of it are encrypted, law enforcement agents are not able to examine the Storage System as ordered in the Search Warrant. The Storage System is comprised of sixteen storage devices. (Banner Aff. ¶ 12). The portions of the Storage System which remain encrypted are

seven Western Digital My Book hard drives (serial numbers WMC1T0358400, WMAZA0052668, WCAVY0868325, WCAZA0078782, WCAZA0078878, WCAPW0572841, WMC1T0276658) and two Maxtor Black Armor external hard drives (serial numbers 2HC04653 and 2HC0491M). (Banner Aff. ¶ 12, 15). The FBI estimates that of the 19.56 Terabytes of information that could be contained in the Storage System, 15.64 Terabytes are encrypted. (Banner Aff. ¶ 19). The Storage System was seized from the residence solely inhabited by Jeffrey Feldman. (Banner Aff. ¶ 12). The seizure of the Storage System was undertaken in complete conformity with the Fourth Amendment; that is, by application to this Court for the Search Warrant after a probable cause showing based upon the proceeds of a thorough investigation. At the time of seizure, the individual units of the Storage System were located in several places around Mr. Feldman's home. *Id.* One of the encrypted Western Digital hard drives was connected to the main computer, two (both encrypted) were located in the living room area, and ten (five of which were encrypted and five of which had been wiped of all data) were located in the bedroom area. *Id.* The two heavily encrypted Maxtor Black Armor external hard drives were located in the pockets of a coat in the closet. *Id.*

This Application seeks an order requiring Jeffrey Feldman to provide agents of the FBI with a decrypted version of contents of the encrypted portions of the Storage System. This could be accomplished by having the encrypted portions of the Storage System available in the courtroom. Upon order of the Court, Jeffrey Feldman could enter the passwords without being observed by law enforcement agents or counsel for the United States, or otherwise provide the unencrypted contents of the Storage System by means agreed upon with the United States. A process like this is the best process possible as it limits the United States' discovery to the previously created documents on Mr. Feldman's computer and does not "[require] him to divulge

through his mental processes his password." *U.S. v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010). The requested order would thus allow the agents to execute the prior search warrant issued by this Court.

III. This Court May Properly Order the Production of the Decrypted Contents under the All Writs Act, 28 U.S.C. § 1651

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

IV. This Court Should Order the Production of the Encrypted Files

Not only does this Court have the authority to compel the production of the decrypted contents of the Storage System, it ought to do so to avoid imposing undue hardships on the United States and on the owner of the Storage System. Further examination of the Storage

system without the order requested in this application, if it is possible at all, would require significant resources and may result in harm to the Storage System itself.

The United States, the FBI in particular, has already expended substantial resources in the effort to break the encryption preventing it from accessing the information as ordered by the Search Warrant and more will be required if the encryption must be broken manually. Members of the FBI's Computer Analysis Response Team ("CART") have spent more than ten weeks working on decrypting Mr. Feldman's storage devices. (Banner Aff. ¶ 20). The FBI's Milwaukee CART contains both agents and specialist "examiners" who are assigned to the FBI. *Id.* The CART having been unsuccessful, the FBI has also enlisted the assistance of the FBI's Cryptologic and Electronic Analysis Unit, which has also spent more than eight weeks attempting to decrypt the Storage System. *Id.* At this time, all of these substantial efforts have been unsuccessful. *Id.*

As encryption becomes more common and more difficult to break, the amount of effort, both in time and resources, required by the FBI to comply with court orders will continue to increase. Encryption is being used more commonly; both by law-abiding, tech-savvy citizens and by sophisticated, computer-based criminals. Stronger encryption protocols are increasingly affordable and available over the internet. Together with the fact that almost all of the data and records being produced today are produced electronically, these realities paint a grim picture of the future for law enforcement officers. 2005 Fed. Cts. L. Rev. 1, I.1 ("More than 99% of new human information now being created and stored is stored electronically."). The FBI is performing admirably in the digital arms race between those seeking to hide evidence of their wrongdoing through encryption and law enforcement officers seeking to uncover that evidence; but the expense in time and resources in investigating cases like this one is beginning to inhibit

the provision of justice. This Court should order the production sought in this Application because it will prevent undue hardship on the efforts of law enforcement to comply with and execute a court-ordered search warrant.

Efforts to manually break the encryption on sophisticated encrypted devices can result in damage to the storage device itself or to the data contained on the storage device, which would place a substantial financial burden on the owner. (Banner Aff. ¶ 21). Up-to-date storage media can be very expensive, but that expense can be negligible in comparison to the value of the data stored on it. Personal data storage systems, such as the one at issue here, can contain a great deal of extremely valuable personal data; entire music collections, expensive pieces of software, financial documents or even, as is more likely in this case, records of inventions and unfiled patents. The data contained on such systems may also be of no financial value, but of great sentimental worth, such as irreplaceable picture and video files. Such important data may be lost during attempts to break encryption for a number of reasons. Some high-security encryption protocols, such as those the FBI believes Mr. Feldman has employed, automatically lock up, erase stored data or even render themselves non-functional if too many incorrect guesses are made at the password. *Id.* Otherwise, if the FBI is unable to decrypt a system using traditional software means they may be required to forcibly remove the micro-processor chips, thus destroying the hardware in the pursuit of the data contained therein. *Id.* The loss of the information on a seized data storage system would not only be a loss to the United States due to the spoliation of evidence, but it could also represent a serious loss to the owner of the system. *Id.* A loss like that can be avoided in this case by ordering Mr. Feldman to bring forward an unencrypted version of the contents of his storage system.

Mr. Feldman needs to be under a judicial order to provide the decrypted contents of the storage system because there need to be legal consequences if he acts in bad faith. Some encryption programs allow only a certain number of guesses at the password before they lock up permanently, delete encrypted contents or cause the destruction of the hardware. If not compelled to decrypt the Storage System's contents by an order from this Court, Mr. Feldman could enter in an incorrect password, thus using up one of a limited number of attempts to unlock the system, and no penalty could be applied for his bad faith. Courts of the United States are empowered to punish "Misbehavior of any person in its presence or so near thereto as to obstruct the administration of justice" and "Disobedience or resistance to its lawful writ, process, order, rule, decree, or command." 18 U.S.C. § 401(1) and (3). The United States believes that the presence of a judicial officer and the issue of a judicial order, along with the surety of punishment should that order be violated, will be sufficient to ensure that Mr. Feldman does not attempt to compromise the sought after evidence during the process of decrypting it. For this reason, it is imperative that Mr. Feldman be ordered to provide the decrypted contents and that the order be carried out in the presence of this Court.

Finally, this Court should order Mr. Feldman to produce the decrypted files because the United States still has probable cause to believe that the contents thereof includes evidence of his violation of 18 U.S.C. 2252A, "Certain activities relating to material constituting or containing child pornography." All of the evidence that originally established the United States' showing of probable cause in support of the Search Warrant is still valid, and the original affidavit and search warrant application are restated and republished in support of this Application. (Banner Aff. ¶ 4). What is more, in the course of their investigation the FBI agents have uncovered additional evidence which lends to the assertion that Mr. Feldman received, possessed,

distributed or produced child pornography. The FBI's forensic analysis of the unencrypted portions of Mr. Feldman's Storage System revealed a large number of user-created links which strongly suggest, often in graphic terms, the presence of child pornography hidden in the encrypted portions of the Storage System. (Banner Aff. ¶ 24, 25). These links could only have been created by the computer's user, and the only person with access to Mr. Feldman's desktop computer was Mr. Feldman himself. (Banner Aff. ¶ 30). During the same forensic analysis, examiners found a peer-to-peer file sharing utility that contained logs of 1009 videos that Feldman had received, distributed and stored. (Banner Aff. ¶ 26). Most of the filenames in the log were unambiguously indicative of child pornography. *Id.* This Court should order the production sought in this Application not just to effectuate the Search Warrant, but to effectuate the purpose of the Search Warrant which was to investigate and prosecute criminal behavior relating to the sexual exploitation of children.

V. Ordering the Production of Decrypted Files would not Offend Mr. Feldman's Fifth Amendment Rights

a. Generally

The Fifth Amendment to the United States Constitution provides, in part, that, "No person … shall be compelled in any criminal case to be a witness against himself." U.S. Const. Amen. V. Recent Supreme Court cases have supported the long-held view that in order to trigger Fifth Amendment protection, the statements sought by the state must be 1) testimonial in nature, 2) compelled by the government, and 3) incriminating. *U.S. v. Hubbell*, 530 U.S. 27, 34-35 (2000). What is more, the Supreme Court has also said that not only must these three aspects exist to trigger Fifth Amendment protection, but that they must be "sufficient." *Baltimore City Dept. of Social Services v. Bouknight*, 493 U.S. 549, 555 (1990) ("The possibility that a production order will compel testimonial assertions that may prove incriminating does not, in all

contexts, justify invoking the privilege to resist production."). In this case, the order applied for by the United States would not trigger Mr. Feldman's Fifth Amendment rights because the creation of the sought information was not compelled by the United States and because anything of testimonial value that could be derived from Mr. Feldman's act of producing the decrypted files is already a foregone conclusion.

b. Compulsion

This Application seeks an order compelling the production of the decrypted contents of a data storage system, but this is not the type of compulsion necessary to trigger one's Fifth Amendment protections. The type of compulsion countenanced in the Fifth Amendment and supporting case law is compulsion at the point of creation. In *Hubbell* the court noted that "relevant to this case is the settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of this privilege. " *Hubbell*, 530 U.S. at 35-36. Moreover, in *Hubbell* the Supreme Court noted that "It is clear, therefore, that respondent Hubbell could not avoid compliance with the subpoena served on him merely because the demanded documents contained incriminating evidence, whether written by others or voluntarily prepared by himself." *Id.*, at 36.

In this case, Mr. Feldman chose to voluntarily prepare the documents himself when he saved files onto the various storage media and the creation of those documents, even if ultimately incriminating, was not compelled, as required by the Fifth Amendment. Mr. Feldman's files were placed on the Storage System at some point prior to the search during which it was seized. When the files were created on the Storage System, there was no government entity or actor forcing Mr. Feldman to do so. This act of creation was entirely the result of Mr. Feldman's own

agency, and so was not "compelled" in the sense required to trigger Fifth Amendment protections. Under the rule from *Hubbell*, Mr. Feldman's creation of the data on the Storage System is an example of incriminating evidence "voluntarily prepared by himself," and it is clear that Mr. Feldman cannot "avoid compliance" with an order from this Court "merely because the demanded documents [contain] incriminating evidence." *Id.* The Fifth Amendment does not protect the incriminating records of Mr. Feldman's criminal conduct because those records were prepared voluntarily and do not meet the "compulsion" requirement for Fifth Amendment protection.

c. Foregone Conclusion

Any implicit testimony that could be drawn from Mr. Feldman's production of the decrypted files is a foregone conclusion, and thus not protected by the Fifth Amendment. Even when, as here, the documents to be discovered are not protected by the Fifth Amendment, the act of producing those documents could, in itself, have sufficient testimonial value to merit Fifth Amendment protections. *Fisher v. U.S.*, 425 U.S. 391, 410 (1976). "The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced." *Id.* However, when the information that could be derived from the act of production is already established to the point of being a "foregone conclusion," that testimonial value is nullified and the Fifth Amendment does not apply. *Id* at 411. "The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "'no constitutional rights are touched.'" *Id* (quoting *In re Harris*, 221 U.S. 274 (1911)). The Seventh Circuit, in applying *Fisher*, noted three "Possible implicit averments inherent in the provision of the

requested documents: that the papers demanded exist, that they are in the possession or control of the taxpayer, and that they are authentic." *U.S. v. Porter*, 711 F.2d 1397, 1400 (7th Cir. 1983).

In the present case, a thorough investigation by FBI agents has established each of the three *Fisher* factors independently of Mr. Feldman's act of production. First, that the files demanded exist is beyond dispute. The files that the United States seeks to have decrypted and turned over are any files which exist on the Storage System. The FBI has independently established, by forensic examination and by reference to the eMule file registry on the unencrypted main computer, that files exist on the hard drive. (Banner Aff. ¶ 15, 23, 24, 25, 26, 28). The United States need not prove more, as the Search Warrant specified that law enforcement officers were to seize and examine all of Mr. Feldman's electronic media. Second, the FBI has proven that the files are within the control of Mr. Feldman by showing that he was the only person who had access to those files. (Banner Aff. ¶ 30). The computer through which Mr. Feldman accessed the Storage System is a desktop computer (as opposed to a mobile, laptop computer) located in his home, where he lived alone. (Banner Aff. ¶ 25, 26, 30). Mr. Feldman was the only person paying taxes at the Premises, was the only person receiving mail, and Mr. Feldman's is the only username present on the Storage System. (Banner Aff. ¶ 30). At the time the Storage System was seized it was in the possession of Mr. Feldman and under his control. (Banner Aff. ¶ 10-12). Third, and finally, authentication is a foregone conclusion because, again, the United States can independently prove that the Storage System belongs to Mr. Feldman. This Application seeks an order in support of the Search Warrant, which directed law enforcement officers to seize and examine any storage media owned by Mr. Feldman at the Premises. That the Storage System is comprised of different storage media is definitional and that they were obtained at the premises is established in the attached affidavit. *Id.* In order, then, to authenticate

the Storage System as what is being sought in the Search Warrant, independent of Mr. Feldman's act of production, the United States must only establish that it belongs to Mr. Feldman, which is concretely proven above.

The Seventh Circuit has never ruled on the issues presented here, but courts in other jurisdictions have applied this rationale to orders requiring the production of decrypted storage media. In *United States v. Fricosu*, 841 F.Supp.2d 1232 (D. Colo. 2012), the court ordered the defendant to decrypt a seized laptop after finding that any disclosure implied by that action was a foregone conclusion. The court in *Fricosu* made this finding based upon a recording of a phone call the defendant had made from jail wherein she admitted that she had a laptop that she had encrypted. *Id,* at 1238; see also *U.S. v. Gavegnano*, 305 Fed.Appx. 954, 956 (4th Cir. 2009) ("Any self-incriminating testimony that [defendant] may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that [he] was the sole user and possessor of the computer."). In *In re Boucher*, 2009 WL 424718 (D.Vt. 2009), the court found that requiring the production of a decrypted hard drive did not trigger Fifth Amendment protection where the defendant had previously shown a border patrol agent images on the computer which the agent suspected to be child pornography. *Id.*

In *In Re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the Eleventh Circuit considered the constitutionality of a decryption order by a lower court and found that the Government in that case had not brought forth enough evidence to prove the existence of the sought after data. 670 F.3d 1335 (11th Cir. 2012). Far from rejecting altogether the sort of order requested in this Application, the *In Re: Grand Jury Subpoena* court seems to endorse the idea, but merely requires that the Government do a thorough investigation and be able to independently prove the *Fisher* factors. *In Re: Grand Jury Subpoena* is easily differentiable

from the present case. In *In Re: Grand Jury Subpoena*, the Government's forensic analyst could not establish that any information existed on the storage media whereas, in this case, the FBI has alleged numerous facts proving that data does exist on the Storage System and, further, that at least some of that data is evidence of child pornography. *Id* at 1340; (Banner Aff. ¶ 15, 23-28). As such, the *In Re: Grand Jury Subpoena* court's requirement that the existence of data on the storage media be independently proven through a thorough investigation is met in this case.

VI. Conclusion

For the aforementioned reasons, the United States respectfully requests an order compelling Jeffrey Feldman to assist in the execution of a federal search warrant by providing federal law enforcement agents a decrypted version of the contents of his encrypted data storage system, previously seized and authorized for search under a federal search warrant, 13-M-421.

Dated at Milwaukee, this 3th day of April, 2013.

JAMES M. SANTELLE
United States Attorney

By:

KARINE MORENO-TAXMAN
Assistant United States Attorney
Karine Moreno-Taxman Bar Number: 1006835
Attorney for Plaintiff
Office of the United States Attorney
Eastern District of Wisconsin
517 East Wisconsin Avenue, Room 554
Milwaukee, Wisconsin 53202
Telephone: (414) 297-1785
Fax: (414) 297-1738
E-Mail: karine.moreno-taxman@usdoj.gov

Alex E. Johnson
Legal Intern
Office of the United States Attorney
Eastern District of Wisconsin
517 East Wisconsin Avenue, Room 554

Milwaukee, Wisconsin 53202
Telephone: (414) 297-1630
Fax: (414) 297-1738
E-Mail: ajohnson9@usa.doj.gov