IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Application for a Search Warrant	)	**Case Number** 17M081
	)	**Magistrate Judge M. David Weisman**

OPINION AND ORDER

The government has presented an application for a search and seizure warrant to seize various items presumed to be located at a particularly identified location (hereinafter "subject premises"). The warrant further requests the authority to seize various items (identified in Attachment B of the warrant application), including various forms of electronic storage media and computer equipment (hereinafter collectively "electronic storage media"). Pursuant to Fed. R. Crim. P. 41(e)(2)(B), the government further requests the authority to remove the electronic storage media from the subject premises, and conduct forensic analysis of these materials at a secure location in a more controlled environment. The Court has reviewed the application and finds that there is sufficient probable cause to conduct a search of the subject premises. Thus, all the aforementioned requests seem justified and appropriate to the Court.

However, in its warrant application, the government also seeks the authority to compel any individual who is present at the subject premises at the time of the search to provide his fingerprints and/or thumbprints "onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the contents of any such device." For the reasons set forth below, this aspect of the search warrant application is denied.

To begin, there are several aspects of the warrant application that are noteworthy. First, the government has plainly established probable cause to believe that someone has been receiving and trafficking child pornography using the subject premises' internet service. Obviously, these are extremely serious allegations. The warrant application makes plain multiple vulnerable victims are, or were, being sexually abused, and someone associated with the subject premises (although as explained below the exact nature of the association is not known) is involved in trafficking these images.

Despite the apparent seriousness of the offenses involved, the Court notes that some of the "boilerplate" background information included in the warrant is a bit dated, such as its explanation that "[t]he internet allows any computer to connect to another computer [so] [e]lectronic contact can be made to millions of computers around the world;" its explanation that a "Blackberry" is a common "Personal Digital Assistant" (*see* ¶ 19); and its suggestion that the use of "cloud technology" is the exceptional way of transferring files and that transferring images to a computer by directly connecting a cable to a camera or other recording device is the expected means of data transfer. (¶ 18.)

The inclusion of this somewhat dated view of technology certainly does not distract from the application's goal of establishing probable cause. However, the dated "boilerplate language" is problematic for what is not included. There is absolutely no discussion of wireless internet service and the possibilities and capabilities that wireless service presents in this context. For example, an unsophisticated internet user, or a careless one, may fail to properly encrypt his wireless service or may share the password injudiciously. Such practices leave open the possibility that it is not an inhabitant of the subject premises that has used the internet to gather and distribute child pornography, but rather it is a person who has access to the internet service at

the subject premises. Obviously, this possibility holds true in all investigations that track the investigation outlined in the instant application. The limitations of this investigation are not fatal to establishing probable cause, but, in the Court's view, these limitations do impact the ability of the government to seek the extraordinary authority related to compelling individuals to provide their fingerprints to unlock an Apple electronic device.

The warrant application also lacks any detailed information about the resident(s) of the subject premises other than the name of the individual who is likely residing there. There is no assertion that the resident has a known link to criminal acts involving child exploitation. There is no testimony from a source linking the resident to trafficking or possessing child pornography. Nor does the warrant application explain what types of internet-accessible hardware are located at the subject premises. Indeed, part of the warrant application states that "it is likely that Apple brand devices" will be found at the subject premises.[1] (¶ 25.) Finally, the warrant application does not identify a comprehensive list of files that the government expects to find on the electronic storage media at the subject premises (or files that can be readily linked to the electronic storage media at the subject premises through other forensic techniques).

The above-noted deficiencies are not surprising. Based on the information contained in the search warrant application, the government's investigation is still developing, and these questions may be answered in the future. As discussed below, however, these factual deficiencies are important for purposes of the Fourth and Fifth Amendment issues presented by this case.

---

[1] Why Apple devices are likely to be found at the premises is not explained. The Court is aware that Apple has a large market share in online hardware, but Microsoft's Windows operating systems continue to dominate the overall market share of operating systems used. *See* Joel Hruska, *Windows Drops Below 90% Market Share for the First Time in Years; Windows 7 Falls Below*, Extreme Tech (Dec. 19, 2016), https://www.extremetech.com/computing/227693-windows-drops-below-90-market-share-for-the-first-time-in-years-windows-7-falls-below-50).

The issues presented in this warrant application are at the cross section of protections provided by the Fourth and Fifth Amendments. Essentially, the government seeks an order from this Court that would allow agents executing this warrant to force "persons at the Subject Premises" to apply their thumbprints and fingerprints to any Apple electronic device recovered at the premises. (*See* Attach. B, ¶ 12.) The request is neither limited to a particular person nor a particular device. And, as noted below, the request is made without any specific facts as to who is involved in the criminal conduct linked to the subject premises, or specific facts as to what particular Apple-branded encrypted device is being employed (if any).

First, the Court finds that the warrant does not establish sufficient probable cause to compel any person who happens to be at the subject premises at the time of the search to give his fingerprint to unlock an unspecified Apple electronic device. The government argues that "there is no Fourth Amendment right implicated by taking a fingerprint."[2] (Gvt. Mem. at 3 n.1) (citing *United States v. Sechrist*, 640 F.2d 81 (7th Cir. 1981)). *Sechrist* does not stand for the simple proposition that "there is no Fourth Amendment right implicated by taking a fingerprint." Indeed, *Sechrist* recognizes that the compelled fingerprinting of a criminal suspect involves two levels of Fourth Amendment analysis. 640 F.2d 81. The *Sechrist* court considered the Fourth Amendment implications of seizing an individual to obtain his fingerprints, and the Fourth Amendment implications of securing the fingerprints themselves. *See id.* at 85 ("The analysis of any Fourth Amendment claim involves a potential violation at two different levels: the 'seizure'

[2]At the Court's request, the government prepared a memorandum of law in support of its warrant application, Government's Memorandum of Law on Compelling Fingerprints to Unlock Encrypted Devices (hereinafter "Gvt. Mem.") The Court appreciates that the government promptly provided this document to support its legal position. Given the short timeframe the government had to prepare this document, the Court recognizes that Gvt. Mem. does not reflect an exhaustive document supporting the government's position. Similarly, this Court, in an effort to timely address the warrant application, has not been able to prepare an opinion that is as exhaustive an exploration of the issues as the Court would prefer to prepare given more time to do so. This Court presented its order to the government for its consideration. Following that exchange, the Court has made minor edits to the opinion and amplified the Fifth Amendment analysis prior to publishing this order.

of the 'person' necessary to bring him into contact with government agents ... and the subsequent search for and seizure of the evidence.") (quoting *United States v. Dionisio*, 410 U.S. 1 (1973)); *see also Davis v. Mississippi,* 394 U.S. 721 (1969) (discussing the potential Fourth Amendment implications of law enforcement attempts to gather fingerprint evidence without regard to the initial seizure necessary to obtain the fingerprints).

Significant to this Court is that the government is seeking "forced fingerprinting" of any person who happens to be at the subject premises -- inclusive of any resident(s) or itinerant visitors. Courts have appropriately and practically recognized that when executing a search warrant, law enforcement officers may detain residents present at the time of the search, *Michigan v. Summers*, 452 U.S. 692 (1981); conduct pat downs of individuals present during the search under the appropriate circumstances, *cf. Ybarra v. Illinois*, 444 U.S. 85 (1979); and sweep the location being searched, *Maryland v. Buie*, 494 U.S. 325 (1990). In some circumstances, these Fourth Amendment intrusions are permitted categorically, *see Muehler v. Mena*, 544 U.S. 93, 98 (2005) (noting that "[a]n officer's authority to detain incident to a search is categorical" in nature), while other Fourth Amendment intrusions are premised on some showing of necessity. *See Ybarra*, 444 U.S. at 91 (stating "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person") (citation omitted); *Buie*, 494 U.S. at 331 (noting distinction between sweeping areas "immediately adjoining the place of arrest" as a matter of course and a broader search based on "articulable facts which, taken together with the rational inferences from those facts, would warrant" a search broader than the immediate area of arrest).

Perhaps most significantly, the *Summers* case, which allows the Fourth Amendment event of seizing occupants of a residence, has been read narrowly by courts to be limited to the

"residents" of the searched premises. *Summers*, 452 U.S. 692. In *Summers*, while police officers were executing a warrant to search a house for narcotics, they encountered respondent on the front steps. *Id.* at 693. The police officers requested Summers' assistance in gaining entry and detained him while they searched the premises. The police found narcotics on the premises and subsequently arrested Summers, searched his person, and discovered heroin in his coat pocket. Respondent was ultimately charged with possession of the heroin found on his person. Summers moved to suppress the heroin found on his person during a search of his home, arguing that the officers had no authority to detain him while they executed the search warrant.

The Supreme Court found that under the Fourth Amendment, police officers have the limited authority to detain an occupant of premises being searched for contraband pursuant to a valid warrant. *Id.* at 705. The Court explained that law enforcement's interest in preventing flight, minimizing harm to officers, and the orderly completion of a search were all justifications for such detention. *Id.* at 702-03. The Court noted that the detention represented "only an incremental intrusion on personal liberty when the search of a home has been authorized by a valid warrant." *Id.* at 704. Thus, seizures of individuals who are present at the time of a search, but are not otherwise connected to the location being searched, are not necessarily subject to temporary detention under *Summers*. *See Panaderia La Diana v. Salt Lake City Corp.*, 342 F. Supp. 2d 1031 (D. Utah 2004); *United States v. Lopez-Garcia*, No. 12-1543 MV, 2013 WL 10093411, at *12 (D.N.M. Dec. 13, 2013).

Finally, to ensure clarity on this issue, the Court is not concerned with the privacy interests of a fingerprint. The courts have made clear that there is no protectable Fourth Amendment interest in the print itself. Rather, it is the method of obtaining the print that is at issue. In *United States v. Guevara-Martinez*, the defendant was stopped and arrested after a

traffic stop resulted in the discovery of narcotics. 262 F.3d 751,752 (8th Cir. 2001). The defendant was transported to the local jail. *Id.* Suspecting he might be an illegal alien, the officers informed the United States Immigration and Naturalization Service of the arrest. *Id.* A day later the defendant was fingerprinted; his fingerprints revealed he was in fact an illegal alien. *Id.* Defendant was indicted for possession with intent to deliver narcotics, but the charge was ultimately dismissed because the traffic stop was found to be illegal. *Id.* A week after the drug charge was dismissed, the defendant was indicted for being an illegal alien. *Id.* The defendant moved to suppress all of the evidence flowing from the illegal traffic stop, including his fingerprints. The Court found his fingerprints were subject to the exclusionary rule. *Id.* at 756. The Court found that "the authorities desired to gather the fingerprints, and were able to take advantage of the unlawful detention in order to get the fingerprints." *Id.* The Court held that "in the absence of evidence that [Defendant's] fingerprinting resulted from routine booking procedures, rather than for the purpose of pursuing [immigration] related proceedings against him" his fingerprints were subject to the exclusionary rule. *Id.* This Court agrees that the context in which fingerprints are taken, and not the fingerprints themselves, can raise concerns under the Fourth Amendment. In the instant case, the government is seeking the authority to seize any individual at the subject premises and force the application of their fingerprints as directed by government agents. Based on the facts presented in the application, the Court does not believe such Fourth Amendment intrusions are justified based on the facts articulated.

Second, and in addition to the Fourth Amendment concerns articulated above, the Court believes that the government's warrant application raises concerns under the Fifth Amendment's protection prohibiting compelled self-incrimination. In its submission, the government argues that "[b]ecause depressing a fingerprint to a device results in no 'testimonial communication' it

does not implicate the Fifth Amendment rights of the user of device . . . Here the finger is like the key to a strongbox, it is not a communication at all, let alone a testimonial one." (Gvt. Mem. at 2) (*citing Commonwealth v. Baust*, 89 Va. Cir. 267 (Cir. Ct. Va. 2014)).

The government is generally correct that the production of physical characteristics generally do not raise Fifth Amendment concerns. *See United States v. Dionisio*, 410 U.S. 1 (1973) (finding a suspect can be compelled to provide a voice exemplar); *Schmerber v. Cal.*, 384 U.S. 757 (1966) (holding a suspect may be compelled to give blood sample); *Gilbert v. Cal.*, 388 U.S. 263, 267 (1967) (finding a suspect may be compelled to provide a handwriting exemplar); *United States v. Wade*, 388 U.S. 218 (1967) (finding a suspect can be compelled to stand in a line up). However, courts have raised Fifth Amendment concerns where the production of information is compelled, and the production itself is deemed incriminating. *See Fisher v. United States*, 425 U.S. 391, 410 (1976) (taxpayer's act of producing documents could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate him). This concern of compelled production often arises in the context of grand jury subpoenas, where the production of requested information may have incriminatory value. *United States v. Doe*, 465 U.S. 605 (1984). Notably, the grand jury subpoena cases do not involve a coexistent Fourth Amendment interest, as courts do not consider an appearance before the grand jury to be a Fourth Amendment event. *See Dionisio*, 410 U.S. 1 ("[A] grand jury subpoena to testify is not [the] kind of governmental intrusion on privacy against which the Fourth Amendment affords protection once the Fifth Amendment is satisfied.") (citation and internal quotations omitted).

In *United States v. Doe*, Defendant Doe was served with a subpoena requiring him to appear before a grand jury and produce encrypted contents located on the hard drives of his

computer and external devices. *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335 (11th Cir. 2012). During the course of a child pornography investigation, the police lawfully seized pieces of Doe's digital media. *Id.* at 1339. The warrant allowed the officers to seize "all digital media, as well as any encryption devices or codes necessary to access such media." *Id.* The forensic examiners were unable to view the encrypted portions of the drive. *Id.* The subpoena ordered Doe to produce the "unencrypted contents" of the digital media and any and all containers or folders thereon." *Id.* Doe invoked his Fifth Amendment privilege against self-incrimination and refused to comply with the subpoena, arguing that by decrypting the contents he would be "testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished." *Id.* at 1339-40. The court stated the issue was not whether contents of the drives themselves were testimonial, but whether "*the act of production* may have some testimonial quality sufficient to trigger Fifth Amendment protection when the production explicitly or implicitly conveys some statement of fact." *Id.* at 1342. In other words, the appropriate question to consider was whether the Government sought testimony implicating the Fifth Amendment by requiring Doe to decrypt certain computer files.

In framing its analysis, the Court of Appeals relied heavily on *Fisher v. United States*, 425 U.S. 391 (1976) and *United States v. Hubbell*, 530 U.S. 27 (2000). In *Fisher*, the IRS required a taxpayer's attorney to hand over various documents including a copy of the taxpayer's returns and an accountant's work papers. *Fisher*, 425 U.S. at 393-94. The attorney refused to turn over the documents, arguing that doing so would violate his Fifth Amendment privilege against self-incrimination. 425 U.S. at 393-94. The Supreme Court disagreed, stating that the act of producing the subpoenaed documents did not involve testimonial self-incrimination because

the Government was "in no way relying on the truth telling of the taxpayer." *Doe*, 670 F.3d 1335 (citing *Fisher*, 425 U.S. at 411). As the *Doe* court explained:

> The [*Fisher*] Court reasoned that, in essence, the taxpayer's production of the subpoenaed documents would not be testimonial because the Government knew of the existence of the documents, knew that the taxpayer possessed the documents, and could show their authenticity not through the use of the taxpayer's mind, but rather through testimony from others. Where the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available.

Id. at 1344 (internal citations omitted). This reasoning has been labeled the "foregone conclusion doctrine."

In contrast, in *Hubbell*, defendant invoked the Fifth Amendment privilege after a grand jury subpoenaed certain documents. 530 U.S. at 30-31. The grand jury indicted Hubell with several federal crimes. *Id.* at 31. Unlike in *Fisher*, the Supreme Court in *Hubbell* found that the act of production was sufficiently testimonial to trigger Fifth Amendment protection because the government had no knowledge of the existence or location of the documents. *Id.* at 45. The *Hubell* Court explained:

> Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it. While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena. The Doe subpoenas also sought several broad categories of general business records, yet we upheld the District Court's finding that the act of producing those records would involve testimonial self-incrimination.

Id. 44-45.

In light of these two opinions, the *Doe* court concluded that an "act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic" and the "touchstone" of whether production is testimonial is if the "government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." *Id.* at 1345 (citing *Curcio v. United States*, 354 U.S. 118, 128 (1957)). The Court explained that an act of production is not testimonial where the government compels merely a physical act, or under the forgone conclusion doctrine, if the government can show with "'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a 'foregone conclusion.'" *Id.* at 1346.

In *Doe*, the government was unaware of what, if any, files existed or the location of the files on the hard drive. *Id.* at 1347. The court found that the government had not shown that it had any prior knowledge of the existence or the location of the files it sought to compel Doe to produce. *Id.* Finally, the Court found requiring Doe to use a decryption password would demand the use of the contents of his mind. *Id.* at 1346.

In the instant case, the government argues that the presentation of a fingerprint is not testimonial because under *Doe v. United States*, 487 U.S. 201 (1987), "[t]o be testimonial, an act must involve communication and 'an accused communication must itself, explicitly or implicitly, relate a factual assertion or disclose information.'" (Gvt. Mem. at 2.) Yet, the connection of the fingerprint to the electronic source that may hold contraband (in this case, suspected child pornography) does "explicitly or implicitly relate a factual assertion or disclose information." *Doe*, 670 F.3d at 1342. The connection between the fingerprint and Apple's biometric security

system, shows a connection with the suspected contraband.[3] By using a finger to unlock a phone's contents, a suspect is *producing* the contents on the phone. With a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.

The government cites *United States v. Wade*, for the proposition that the Fifth Amendment privilege against self-incrimination offers no protection against compulsion to submit to fingerprinting. (Gvt. Mem. at 2) (citing *Wade*, 388 U.S. 218, 223). This case, however, was decided in 1967, prior to the existence of cell phones, and in the context of utilizing fingerprinting solely for identification purposes. In the context of the Fifth Amendment, this Court finds these two starkly different scenarios: using a finger print to place someone at a particular location, or using a fingerprint to access a database of someone's most private information. The *Wade* court could not have anticipated the creation of the iPhone nor could it have anticipated that its holding would be applied in such a far-reaching manner. In fact, the Supreme Court has said "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

The societal concerns of privacy raised in *Riley* provide an important backdrop to the issue presented in the instant case. The *Riley* court recognized that the modern day cell phone, based in part on the personal and intimate information regularly stored on such devices, is

[3] The strength and depth of that connection may still be at issue, but connecting a suspect to contraband via biometric evidence is a large step forward in the criminal investigatory process.

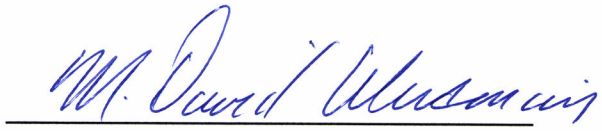
subject to higher Fourth Amendment protections than other items that might be found on a person. *Id.* at 2485. The considerations informing the Court's Fourth Amendment analysis of a cell phone's role in modern day life, we believe raise Fifth Amendment concerns as well. We do not believe that a simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life (and potentially provides direct access to contraband) is supported by Fifth Amendment jurisprudence.

In closing, upon presentation of the warrant application to this Court, the government identified for this Court that the warrant application was seeking the forced fingerprinting discussed herein. The government further noted "[t]his is the language that we are making standard in all of our search warrants." This declaration of standardization is perhaps the crux of the problem. As the Court hopes it is plain from the above, the issues presented here require a fact-intensive inquiry both for purposes of the Fourth Amendment and the Fifth Amendment. This opinion should not be understood to mean that the government's request for forced fingerprinting will always be problematic. In circumstances where the existence and nature of the electronic information sought is a "foregone conclusion," Fifth Amendment jurisprudence tells us that the concerns noted above may be obviated. Similarly, under Fourth Amendment jurisprudence where there is an individualized showing more firmly establishing a connection between an individual and criminal conduct, the Fourth Amendment concerns raised herein may fall to the wayside. Indeed, after the execution of this warrant, the government may garner additional evidence that addresses both of these concerns such that the government can promptly apply for additional search warrants. We simply are not there yet.

For the reasons stated, the Court does not find, under the circumstances presented here, that the government has established a proper basis to force any individual at the subject premises to provide a fingerprint or thumbprint in an attempt to unlock any Apple device that may be found.

SO ORDERED.

ENTERED: February 16, 2017



M. David Weisman
United States Magistrate Judge