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

In the Matter of the Search of:	)	
	)	
The single-family home and attached garage located at [redacted]	)	**Magistrate Judge Sheila Finnegan**
	)	**17 M 85**
	)	
	)	**UNDER SEAL**
	)	

ORDER

The government has presented an Application for a warrant under Federal Rule of Criminal Procedure 41(c) to search a single-family home and attached garage (the "Subject Premises"), and seize evidence, instrumentalities, and contraband concerning the possession and receipt of child pornography. Since the materials to be seized (described in Attachment B) may reside on a computer, smartphone, iPad or other electronic device within the Subject Premises, the government also requests authority to remove the electronic devices and storage media for a thirty-day period, and conduct forensic analysis at a secure location in a more controlled environment. The Court has reviewed the Application and finds that there is probable cause for the above search and seizure.

The reason for this Order is that the Application also seeks authority for what amounts to a separate seizure of four named individuals associated with the Subject Premises. All have the same last name and appear to be a family: father, mother, and two adult sons. The supplemental seizure is described as follows:

> I request that the Court authorize law enforcement to press the fingers (including thumbs) of [the four named persons] at the Subject Premises to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the Subject Premises for the purpose of attempting to

> unlock the device via Touch ID in order to search the contents as authorized by the requested warrant.

(Application ¶ 41). At present, the government has no information as to whether Apple devices will be found within the Subject Premises and, if so, to whom they belong. As the Application recognizes, it "may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device." (*Id*. ¶ 40).

For reasons discussed below, the Court denies authorization for this seizure of the four individuals. As Magistrate Judge Weisman noted in a recent case, when authority is sought not only to search electronic devices but also to force individuals to press their fingers to the devices to unlock them, this raises seizure issues "at the cross section of protections provided by the Fourth and Fifth Amendments." *In re Application for a Search Warrant*, 17 M 81, at 3 (N.D. Ill. Dec. 20, 2016). In the pending case, the government has established probable cause to search the devices, and seeks authority to use force only against four specific persons associated with the Subject Premises if present during the search. Consequently, this scenario does not present the same Fourth Amendment concerns that Magistrate Judge Weisman identified in *In re Application for a Search Warrant* where the government sought authority to exert force as to *any* person who happened to be at the subject premises during the search. *Id*. at 5-6.

This does not, however, end the analysis in determining whether the forced fingerprinting would be lawful under the Fifth Amendment. In *Fisher v. United States,* 425 U.S. 391 (1976), the Supreme Court held that a compelled act of production may be testimonial and in violation of an individual's Fifth Amendment right against self-

incrimination where the act "tacitly concedes" that the produced materials exist and are in the possession or control of the individual. *Id*. at 410. Under the circumstances presented here, the compelled act (the entry of a biometric passcode using finger or thumb) may unlock the device, thereby producing its contents to the government.[1] This act of production would implicitly communicate potentially incriminating information currently unknown to the government. For example, if an iPhone is found at the Subject Premises that turns out to contain child pornography and it is unclear to whom the device belongs, the individual whose finger unlocks the iPhone will implicitly communicate that he controls and possesses that device and the contraband stored within it.

The government does not seek authority to force the individuals to enter passcodes into the devices if necessary to unlock them, apparently recognizing that this would violate the Fifth Amendment. It is only if the Apple device has been configured in advance to unlock in response to the individual's unique fingerprint (the biometric passcode), that the government asserts the Fifth Amendment does not apply. In its view, law enforcement would be compelling a mere physical act rather than a communicative act. This Court disagrees, since the implicit testimony resulting from the compelled act of unlocking the device is the same whether the individual is required to do so by entering a numeric passcode or touching his finger to the sensor. Therefore, the Court denies (for now) the government's request for authority during the search to

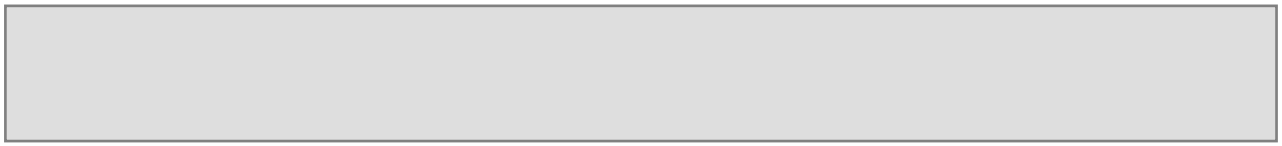
[1] Biometrics authentication "is used in computer science as a form of identification and access control. . . . Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. . . . Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods." WIKIPEDIA, https://en.wikipedia.org/wiki/Biometrics (last visited January 30, 2017) (citations omitted).

force the fingers and thumbs of any of the four individuals to Apple devices. Without evidence demonstrating that a specific Apple device belongs to the specific individual who will be forced to unlock it (making the testimonial aspect of the production a foregone conclusion), the compelled act would violate the Fifth Amendment.

A. BACKGROUND

The FBI has developed evidence that someone associated with the Subject Premises opened a account in and then used it to access and store child pornography. On the account in question was accessed using an iPhone 5. Most recently, the account was accessed using an iPad 2 It is still unclear who used the

account to download and store child pornography. four individuals list the Subject Premises as their residence If they are present during the search, the government seeks authority to force their fingers or thumbs to any Apple devices that are found.



According to the government, some models of Apple devices (including iPhones and iPads – both of which were at times used to access the [redacted] account) offer a feature called "Touch ID." This allows users to unlock the device using a fingerprint or thumbprint in lieu of entering a passcode. (Application ¶¶ 34, 35). A user who enables Touch ID on a device may register up to 5 fingerprints (their own or others) to be used to unlock the device. Users commonly choose a thumb or index finger. Touch ID is considered not only a more convenient manner of unlocking the device but also a more secure way of protecting the contents. (*Id*. ¶ 36). Even if Touch ID is enabled, the user must enter the passcode under certain circumstances: (a) if more than 48 hours have passed since the device was last unlocked; (b) if the device was remotely locked; (c) if the device has been turned off or restarted; and (d) after five unsuccessful attempts to unlock the device via Touch ID. (*Id*. ¶ 37). Some models of Apple devices encrypt the data stored on the device so law enforcement will likely be unable to search a locked device. (*Id*. ¶ 38).

B. ANALYSIS

1. Act of Production is Testimonial

Under the Fifth Amendment, no person "shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. Courts have construed the word "witness" to mean "a person who provides testimony." *See United States v. Hubbell*, 530 U.S. 27, 49 (2000) (Thomas, J., concurring). Therefore, the Fifth Amendment "protects a person . . . against being incriminated by his own compelled

testimonial communications." *Fisher*, 425 U.S. at 409. Put another way, the Fifth Amendment is implicated if the communication is compelled, testimonial, and incriminating in nature. *Id.* at 408; In *re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1341 (11th Cir. 2012). In deciding whether the forced unlocking of Apple devices using a biometric passcode (a finger or thumb) is testimonial under the circumstances presented here, the Court begins by examining a trilogy of Supreme Court decisions.

a. *Fisher v. United States* (1976)

The Supreme Court recognized in *Fisher v. United States* that the act of producing documents to the government "has communicative aspects of its own, wholly aside from the contents of the papers produced." 425 U.S. at 410. Specifically, "[c]ompliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena." *Id*. *Fisher* involved IRS summonses for tax return working papers prepared by the taxpayers' accountants that the IRS already knew were in the possession of the taxpayers' attorneys (delivered to them by the taxpayers).

In considering the Fifth Amendment issue, the *Fisher* Court closely examined the specific facts before it, including whether the government was "relying on the 'truth-telling' of the taxpayer to prove the existence of or his access to the documents." *Id.* at 411. The Court concluded that the answer was "no," since "[t]he 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."

Id. This was so, the Court reasoned, because "[t]he papers belong to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on the tax returns of his client." Fisher, 425 U.S. at 411. Under these circumstances, the Court found that enforcement of the IRS summons did not violate the Fifth Amendment, since "[t]he question is not of testimony, but of surrender." *Id*.

b. *United States v. Hubbell* (2000)

The Supreme Court came to a different conclusion twenty-four years later, in *United States v. Hubbell*, stating that "[w]hatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it." 530 U.S. at 44. In response to a subpoena, Hubbell had produced numerous categories of documents to the grand jury only after being granted immunity, yet was later indicted on new charges based on those documents. The government argued that the grant of immunity did not preclude derivative use of the produced documents because its "possession of the documents [was] the fruit *only* of a simple physical act-the act of producing the documents." *Id*. at 43 (emphasis in original).

In determining whether the criminal charges should be dismissed for violating Hubbell's Fifth Amendment rights, the Court reaffirmed the holding in *Fisher*: "We have held that 'the act of production' itself may implicitly communicate 'statements of fact.' By 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.'" *Id*. at 36. The Court further explained that "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Id*. at 36 n.19. Indeed, "[c]ompelled testimony that communicates

information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory." *Id.* at 38 (citing *Doe v. United States*, 487 U.S. 201, 208 n.6 (1988)). This is so because "[i]t is the Fifth Amendment's protection against the prosecutor's use of incriminating information derived directly or indirectly from the compelled testimony of the respondent that is of primary relevance . . ." *Id*.

Unlike in *Fisher*, however, the *Hubbell* Court found that the implicit testimony from the act of production was *not* a foregone conclusion. It noted that 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." *Id.* at 44-45. In contrast, in *Hubbell*, "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." *Id*. at 45. Thus, the Court found that Hubbell's act of production "had a testimonial aspect, at least with respect to the existence and location of the documents sought by the Government's subpoena," and he "could not be compelled to produce those documents without first receiving a grant of [use and derivative use] immunity under [18 U.S.C.] § 6003." *Id*. Since the government apparently was unable to prove that the evidence used to obtain the indictment was derived from wholly independent sources, the indictment was dismissed.[4]

[4] In explaining why derivative use immunity was necessary, the Court described how the subpoena had required Hubbell to identify the hundreds of documents responsive to specific requests in the subpoena, stating:

> [W]e cannot accept the Government's submission that [Hubbell's] immunity did not preclude its derivative use of the produced documents because its "possession of the documents [was] the fruit *only* of a simple physical act-the act of producing the documents." [Brief for United States] at 29. It was

c. *Doe v. United States* (1988)

In a third seminal case (predating *Hubbell*), *Doe v. United States*, the compelled act was of a different nature. The government served subpoenas not on the grand jury target who invoked the Fifth Amendment but on foreign banks (with branches in the U.S.). 487 U.S. at 203. The subpoenas commanded the banks to produce records of accounts over which Doe (the target) had signatory authority. *Id.* Citing bank-secrecy laws in the foreign countries, the banks refused to comply without customer consent. The government then sought a court order requiring Doe to sign forms "consenting to disclosure of any bank records respectively relating to 12 foreign bank accounts over which the Government knew or suspected that Doe had control." *Id*. After the motion was denied as violating the Fifth Amendment, the government revised the consent directive and sought reconsideration. This time the forms "purported to apply to any

---

> unquestionably necessary for respondent to make extensive use of "the contents of his own mind" in identifying the hundreds of documents responsive to the requests in the subpoena. *See Curcio v. United States*, 354 U.S. 118, 128 (1957); *Doe v. United States*, 487 U.S. at 210. The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox. *Id.* at 210, n.9. The Government's anemic view of respondent's act of production as a mere physical act that is principally nontestimonial in character and can be entirely divorced from its "implicit" testimonial aspect so as to constitute a "legitimate, wholly independent source" (as required by *Kastigar* [*v. United States*, 406 U.S. 441 (1972)]) for the documents produced simply fails to account for these realities.

Hubbell, 530 U.S. at 43. It is worth noting that where the government obtains documents by search warrant rather than subpoena, it is law enforcement who examines the universe of materials and decides which documents (or other items) are within the warrant's scope and so may be seized. As a result, the compelled act of production (here the unlocking of a device that produces the contents for the search) tacitly concedes only the individual's possession and control of the device and its contents – not the existence, location, authenticity, and responsiveness of documents, as where an individual produces documents in response to a subpoena. Given this, one could argue that the foregone conclusion exception is satisfied by pre-existing evidence of the individual's possession and control of the device (not more), and that absent such evidence, the government must grant immunity for the compelled act of production but not the derivative use of the seized contents. The Court need not decide these issues at this time.

and all accounts over which Doe had a right of withdrawal, without acknowledging the existence of any such account." *Id.* at 204.

In considering whether the compelled act of signing the forms was testimonial and so protected by the Fifth Amendment, the Court said it needed to focus on the particular facts and circumstances before it. *Id*. at 214-15 (citing *Fisher*, 425 U.S. at 410). Based on the careful manner in which the consent directive was drafted, the Court then concluded that "neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information to the Government." *Id*. at 215. The Court's reasoning is quoted at length below, since the government in the case at hand relies on some of this analysis for its position that the forced touching of fingers to Apple devices would compel only physical and not testimonial acts.

> The consent directive itself is not "testimonial." It is carefully drafted not to make reference to a specific account, but only to speak in the hypothetical. Thus, the form does not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner. Nor does the form indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist. [Citations omitted].
>
> The form does not even identify the relevant bank. Although the executed form allows the Government access to a potential source of evidence, the directive itself does not point the Government toward hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence. The Government must locate that evidence "'by the independent labor of its officers[.]'" . . . As in *Fisher*, the Government is not relying upon the "'truthtelling'" of Doe's directive to show the existence of, or his control over, foreign bank account records. . . .
>
> Given the consent directive's phraseology, petitioner's compelled act of executing the form has no testimonial significance either. By signing the form, Doe makes no statement, explicit or implicit, regarding the existence of a foreign bank account or his control over any such account. Nor would his execution of the form admit the authenticity of any records produced by the bank. . . . Not only does the directive express no view on the issue, but because petitioner did not prepare the document, any statement by

> Doe to the effect that it is authentic would not establish that the records are genuine. . . . Authentication evidence would have to be provided by bank officials. Finally, we cannot agree with petitioner's contention that his execution of the directive admits or asserts Doe's consent. The form does not state that Doe "consents" to the release of bank records. Instead, it states that the directive "shall be construed as consent" with respect to Cayman Islands and Bermuda bank-secrecy laws. Because the directive explicitly indicates that it was signed pursuant to a court order, Doe's compelled execution of the form sheds no light on his actual intent or state of mind. The form does "direct" the bank to disclose account information and release any records that "may" exist and for which Doe "may" be a relevant principal. But directing the recipient of a communication to do something is not an assertion of fact or, at least in this context, a disclosure of information. In its testimonial significance, the execution of such a directive is analogous to the production of a handwriting sample or voice exemplar: it is a nontestimonial act. In neither case is the suspect's action compelled to obtain "any knowledge he might have." [*United States v.*] *Wade*, 388 U.S. [218,] 222 [(1967)].
>
> We read the directive as equivalent to a statement by Doe that, although he expresses no opinion about the existence of, or his control over, any such account, he is authorizing the bank to disclose information relating to accounts over which, in the bank's opinion, Doe can exercise the right of withdrawal. . . . When forwarded to the bank along with a subpoena, the executed directive, if effective under local law, will simply make it possible for the recipient bank to comply with the Government's request to produce such records. As a result, if the Government obtains bank records after Doe signs the directive, the only factual statement made by anyone will be the bank's implicit declaration, by its act of production in response to the subpoena, that it believes the accounts to be petitioner's. . . . The fact that the bank's customer has directed the disclosure of his records "would say nothing about the correctness of the bank's representations."

Id. at 215-18 (citations and footnotes omitted).

In response to a hypothetical raised in the dissent, the *Doe* majority also opined that compelling execution of the consent directive was more like "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it is like "be[ing] compelled to reveal the combination to [petitioner's] wall safe." *Id*. at 210 n.9.[5]

[5] In his dissent, Justice Stevens said a suspect "may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed." *Doe*, 487 U.S. at

The majority also relied on the line of cases that have "distinguished between the suspect's being compelled himself to serve as evidence [which was permissible] and the suspect's being compelled to disclose or communicate information or facts that might serve as or lead to incriminating evidence[,]" which violated the Fifth Amendment. *Id*. at 211 n.10 (citing *Schmerber v. California*, 384 U.S. 757, 764 (1966) (drawing suspect's blood without consent to measure blood alcohol content did not involve forcing him to communicate) and *Holt v. United States*, 218 U.S. 245, 252-53 (1910) (suspect forced to put on blouse for witness to see whether it fit)).

2. Compelled Act of Placing Finger to Apple Device

In the almost thirty years since *Doe* was decided, technology has evolved at a dramatic pace, creating the need to apply the holdings, analysis, and hypotheticals from the Supreme Court's trilogy of now dated act-of-production cases to facts likely never imagined at the time. In the pending case, the compelled act--the forced placement of a finger to the touch pad of an Apple device--will not require the individuals to use their minds to decide whether particular documents fall within the categories set forth in a subpoena and so must be produced (as in *Hubbell*). Here, the entirety of the contents of the devices will be produced when the devices are unlocked. The government will then conduct its own search of all the content to determine whether any materials fall within the list of items described in Attachment B to the warrant. Nor do the individuals even need to select which fingers or thumbs to press to the devices since law enforcement intends to choose. Nonetheless, if an individual's finger succeeds in unlocking a device containing child pornography, then this act of production will clearly

219. Justice Stevens explained that "[t]he forced execution of a document that purports to convey the signer's authority . . . does invade the dignity of the human mind; it purports to communicate a deliberate command." *Id*. at 219 n.1.

communicate incriminating and unknown information to the government beyond what is learned from the examination of the materials on the device. At the very moment of unlocking the device using a unique fingerprint, the individual "tacitly concedes" that the device and its contents are in his "possession or control". *Fisher,* 425 U.S. at 410.

Far different was the situation in *Doe* where the act of signing the consent directive was *not* testimonial, since the documents were to be produced by foreign banks (not Doe), and the language in the directive was watered down to avoid linkage between Doe and the accounts. Under these circumstances, the Supreme Court concluded that Doe made "no statement, explicit or implicit, regarding the existence of a foreign bank account or his control over any such account." 487 U.S. at 215-16. And even if the banks accepted the consent and produced records in response, the *Doe* Court said the implicit factual statement was only from the bank (that *it* believed the accounts to be Doe's). In contrast, in the pending case, the implicit factual statement is undoubtedly coming from the four individuals rather than a separate entity. If one of them succeeds in unlocking an Apple device, there is no divorcing the compelled act of production from the resulting implicit testimony that he possesses and controls the device and any contraband or evidence stored on it. Indeed, since the unlocking occurs at the exact moment when the individual presses his unique fingerprint to the device, the connection is direct and powerful.

While the government has not submitted a written memorandum in support of the issuance of the warrant, the Assistant U.S. Attorneys have explained their position that the act of touching the finger to a device is a physical rather than testimonial act, much like giving a fingerprint. Further, they observe that the individuals will not need to use or

reveal what is in their minds, as in *Fisher* and *Hubbell* where subpoenas were served seeking categories of documents. When law enforcement officers select a finger or thumb and place it on the touch pad of a device to unlock it, they view this as analogous to requiring someone to surrender a key to a strongbox, where the Fifth Amendment has no application.

Wisely, the Supreme Court recognized over forty years ago in *Fisher* that questions regarding whether an act of production is both testimonial and incriminating "perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof." 425 U.S. at 410. More recently, the Supreme Court has also cautioned (in the Fourth Amendment context) against mechanically applying categorical rules without considering the rationale for such rules in the context of new technology. *Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (rejecting government's request to extend search incident to arrest doctrine to allow warrantless searches of cell phones, stating "a mechanical application of [*United States v*.] *Robinson*[, 414 U.S. 218 (1973)] might well support the warrantless searches at issue here. But while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.").[6] *See also*

[6] Writing for the majority in *Riley,* Chief Justice Roberts observed that the modern cell phones recovered during the searches incident to arrest in that case were "based on technology nearly inconceivable just a few decades ago, when *Chimel* [*v. California*, 395 U.S. 752 (1969)] and *Robinson* were decided." 134 S. Ct. at 2484. The Court was thus critical of the government's position that "a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items." *Id*. at 2488 (citation omitted). According to the Court, this was "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Id*. In explaining the difference here, the Court said "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of

Missouri v. McNeely, 133 S. Ct. 1552, 1564 (2013) ("While the desire for a bright-line rule is understandable, the Fourth Amendment will not tolerate adoption of an overly broad categorical approach that would dilute the warrant requirement in a context where significant privacy interests are at stake."). This Court is also mindful that "[i]t has been repeatedly decided that [the Fifth Amendment] should receive a liberal construction, so as to prevent stealthy encroachment upon or 'gradual depreciation' of the rights secured by [it], by imperceptible practice of courts or by well intentioned but mistakenly over-zealous executive officers." *Fisher*, 425 U.S at 417 (Brennan, J., concurring) (quoting

---

a cigarette pack, a wallet, or a purse." *Id.* at 2488-89. The Court continued: "A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom. Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* at 2489. In reaching its holding, the Court also considered the pervasiveness of modern cell phones and their enormous storage capacity:

> But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos.
>
> * * *
>
> Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.
>
> * * *
>
> Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Id. at 2489-91 (citations omitted). While acknowledging that its decision to deny automatic warrantless searches of cell phones incident to arrest "will have an impact on the ability of law enforcement to combat crime[,]" given the prevalent use of cell phones within criminal enterprises, the Court recognized that "[p]rivacy comes at a cost." *Id*. at 2493.

Gouled v. United States, 255 U.S. 298, 304 (1921)). *See also Maness v. Meyers*, 419 U.S. 449, 461 (1975).

Here, the government's position that the compelled act may be categorized as physical and so is not testimonial under the Fifth Amendment has only superficial appeal. Ultimately it cannot be squared with the Supreme Court's rationale for granting protection to certain acts of production: avoiding the compelled testimonial aspects of such acts. What the trilogy of Supreme Court cases teaches is that the fundamental question in determining whether a compelled act of production is "testimonial" is whether, under the specific facts and circumstances presented, the act implicitly conveys incriminating information unknown to the government. In the digital era and with the advent of biometrics, an individual--with a touch of a finger--is now able to produce the entire (often vast) contents of a computer device such as a smartphone. More significantly, the individual necessarily communicates information to the government when he unlocks the device and thereby produces the contents: that he has accessed the device before (at a minimum to set up the biometric passcode), and currently possesses and controls the device and its contents.

Assuming the device contains contraband, the incriminating communication will be both direct and immediate. There will be no need for a third party's analysis to convert the act of production into incriminating evidence, as when a fingerprint compelled from a suspect for identification purposes is sent to a lab to compare with prints from a crime scene. Advances in technology designed to make the Apple device more secure and convenient allow configuration so a unique fingerprint may serve as a proxy for entry of a passcode. While the method of unlocking the device is different

(using a biometric passcode in lieu of a numeric passcode), the implicit testimony resulting from the unlocking of the device is unchanged.

Plainly, this implicit testimony would not be a foregone conclusion under the circumstances presented here. Instead, the testimony conceivably could be crucial to a prosecution, especially when there are four adults associated with the Subject Premises, [redacted] If all four individuals are present during the search and decline to answer questions, such as identifying the owner of an iPhone located in a common area of the house, the government may find it challenging to determine to whom the device belongs. But if law enforcement officers forcibly place the index fingers of the [redacted] to this device, and it unlocks upon the touch of one but not the other, revealing hundreds of images of child pornography, the value of the implicit testimony from the compelled act is obvious. While no privilege attaches to the pre-existing pornographic images on the device, the individual in this scenario is being compelled to implicitly testify that he possesses and controls the device and the contraband stored on it. Indeed, since possession of such child pornography is itself a criminal act, one could argue that the compelled act even demonstrates criminality.

For these reasons, unless the implicit testimony from the act of unlocking a device would be a foregone conclusion, or the government grants immunity for the act of production, this Court believes the Fifth Amendment prohibits the forced unlocking of

a device by finger touch. As one commentator aptly explained, it is not persuasive to label the use of a biometric passcode as "physical evidence" rather than "communicative evidence" and deny Fifth Amendment protection on this basis:

> The two categories of interpretation used by the Court have been more of [a] guide rather than a strict classification system, and the Supreme Court has admitted that each situation must be examined on a case-by-case basis. A biometric password such as a fingerprint does not fit neatly into either category, but an examination of the logic developed by the Supreme Court in precedential cases suggests that a fingerprint, when used as a password rather than as a method of identification, possesses the testimonial qualities that should entitle it to the Fifth Amendment privilege against self-incrimination.

See Kara Goldman, Note, *Biometric Passwords and the Privilege Against Self-Incrimination*, 33 CARDOZO ARTS & ENT. L.J. 211, 216, n.8 (2015).[7]

3. Lower Court Cases

Neither the Supreme Court nor the Seventh Circuit has yet examined a Fifth Amendment claim in a case involving locked or encrypted computer devices. Some lower courts have done so, most commonly in child pornography cases where data on previously-seized computers or hard drives turned out to be password protected or encrypted. The government then served grand jury subpoenas or court orders to compel production of the decrypted devices or hard drives, or to compel entry of the passcode directly into the device to decrypt the contents. As noted below, these courts have held that the compelled acts conveyed implicit testimony so were permissible only where the foregone conclusion exception applied or full immunity was granted. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346 (court declined to compel compliance with grand jury subpoena requiring Doe to produce

[7] For another thorough discussion of the issues, see Matthew J. Weber, Note, *Warning -- Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, 2016 U. ILL. J.L. TECH. & POL'Y 455 (Fall 2016).

decrypted hard drives, since immunity was given only for the act of production, which act was "tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files"; that testimony was not a foregone conclusion). *See also In re Boucher*, No. 2:06–MJ–91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (court denied motion to quash grand jury subpoena requiring entry of passcode into computer seized at border; foregone conclusion exception applied since Boucher already had admitted possession of, and provided access to, the computer from which agents viewed child pornography); *Com. v. Gelfgatt*, 468 Mass. 512, 523, 11 N.E.3d 605, 615 (2014) ("[F]actual statements that would be conveyed by the defendant's act of entering an encryption key in the computers are 'foregone conclusions' and, therefore, the act of decryption is not a testimonial communication that is protected by the Fifth Amendment."); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012) (Fifth Amendment not implicated by requiring production of unencrypted contents of computer files since foregone conclusion exception applied).[8]

Only two lower court cases have examined the Fifth Amendment implications of the forced unlocking of a device by finger touch: *State v. Diamond*, __ N.W.2d __, 2017 WL 163710 (Ct. App. Minn. Jan. 17, 2017), and *Com. v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635 (Cir. Ct. Va. 2014). Both held that there was no Fifth Amendment

[8] The Third Circuit will soon decide a case where the suspect in a child pornography investigation is being held in contempt for violating an order under the All Writs Act (28 U.S.C. § 1651), requiring him to enter passcodes into previously-seized computers in order to decrypt the files. *In the Matter of the Search of Seized Items*, 2:15-MJ-850-CMR, Doc. 21 (E.D. Pa. Oct. 5, 2015), *appeal docketed sub nom. U.S. v. Apple Mac Pro Computer*, No. 15-3537. The oral argument on September 7, 2016 is available at https://www.courtlistener.com/audio/24617/united-states-v-apple-macpro-computer/ (last visited February 17, 2017).

protection for this compelled act. Neither is persuasive since they labeled the unlocking act as "physical" and ignored the implicit testimony conveyed from the compelled act. The cases are also distinguishable; both involved orders to unlock specific smartphones that the government had seized from the persons who were later compelled to unlock them, and those persons did not appear to dispute that they possessed and controlled the phones prior to seizure.

In applying the foregone conclusion exception in *Baust*, the court inexplicably focused on whether the *passcode* (rather than Baust's possession and control of the device) was a foregone conclusion. Finding that the "password is not a foregone conclusion," the court held that the Fifth Amendment prohibited compelled disclosure of the passcode itself. But the court said there was no Fifth Amendment issue with compelling the forced unlocking of the device by finger touch since this was a mere physical act that did not require any knowledge. 2014 WL 10355635, at *4.

In *Diamond,* it does not appear that the person compelled to unlock the smart phone by finger touch ever argued that this would be a tacit acknowledgement of his possession and control of the phone and its contents. Instead, Diamond argued only that the forced unlocking "effectively required him to communicate 'that he had *exclusive use* of the phone containing incriminating information.'" 2017 WL 163710, at *6 (emphasis added). The court dismissed this out of hand for two reasons. First, the unlocking of the device was a physical act rather than testimonial. *Id*. Second, there was "no support" for the assertion that "only his fingerprint would unlock the cellphone or that his provision of a fingerprint would communicate his exclusive use of the cellphone." *Id*.

In a third case, *State v Stahl*, 206 So.3d 124, 2016 WL 7118574 (Fla. App. 2d Dist. Dec. 7, 2016), the court was uncertain what the motion to compel "production" of the passcode meant: telling law enforcement the passcode; directly entering the passcode into the device; or touching a finger to the device to unlock it. According to the opinion, the State filed the motion after Stahl "refused to give law enforcement the passcode." *Id*. at 128. He initially identified his cellphone, said it was in his residence, and gave consent to search it but changed his mind after officers retrieved the phone from the residence. *Id.* The record in the lower court did not indicate, however, whether the officers "had attempted to compel Stahl to unlock the phone using his fingerprint[,]" (*id*. at 130 n.5), or sought to make him testify to the passcode or enter it into the iPhone. (*Id*. at 133 n.9). Regardless, the appellate court concluded that the lower court had erred in denying the motion for production of the passcode on Fifth Amendment grounds since the foregone conclusion exception was satisfied. In applying that exception, the court said the government needed to show only its knowledge of the existence of the passcode (not the actual passcode), Stahl's control or possession of the passcode, and the self-authenticating nature of the passcode. *Id.* at 136.

In dicta, the court went on to question, however, whether the Fifth Amendment actually applied to the compelled unlocking of a device in *any* manner. Given "technology advances," the court said it questioned the "continuing viability" of a distinction between "identifying the key that will open the strongbox" and "telling an officer the combination." *Id.* at 135. Since compelling an individual to unlock a device by fingerprint was a mere physical act so not protected, the court said the Fifth

Amendment also did not protect "individuals who passcode protect their iPhones with letter and number combinations…." *Id.* at 135.

As the above discussion of lower court cases demonstrates, there has been considerable variation in how courts have analyzed the Fifth Amendment issues and applied the foregone conclusion doctrine in these computer decryption and unlocking cases. In any event, none of the cases involved a situation like the one presented here where the government does not yet possess (and cannot specifically identify) the devices to be unlocked, and has *no evidence* linking a specific device to any of the four individuals who would be compelled to unlock it. As noted, in virtually all of the prior cases, the government had the device in hand when it sought the compulsion order, and appeared to have ample evidence demonstrating the compelled person's possession and control of the device so did not need evidence of this. The same cannot be said in the pending case where the government acknowledges that it currently lacks such evidence.

C. CONCLUSION

As the Supreme Court observed in *Fisher,* questions regarding whether an act of production is testimonial do not lend themselves to "categorical answers" and "their resolution may instead depend on the facts and circumstances of the particular cases…." 425 U.S. at 410. In resolving the question here, the fundamental question must be whether, under the circumstances presented, the compelled act of production implicitly conveys incriminating information to the government that is not a foregone conclusion, namely, that the individual possesses and controls the Apple device and its contents. Since the answer is undoubtedly "yes," this Court believes that--absent a

grant of immunity for the act of production—the four individuals may not lawfully be compelled to unlock unspecified Apple devices during the search of the Subject Premises. For these reasons, the Court denies the government's request for authorization to exert force to compel the individuals to unlock any devices during the search.

ENTER:

Dated: February 21, 2017

SHEILA FINNEGAN
United States Magistrate Judge