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

In the Matter of the Search Warrant Application for [redacted]	)	
	)	**UNDER SEAL**
	)	
	)	Case No. 17 M 85
	)	
	)	Judge Edmond E. Chang

MEMORANDUM OPINION

The United States seeks review of the magistrate judge's denial of one aspect of the government's search-warrant application in this investigation: authorization to require the four residents of a home to apply their fingers and thumbs (as chosen by government agents) to the fingerprint sensor on any Apple-made devices found at the home during the search. Ordinarily, review of the magistrate judge's decision on a warrant application would be *ex parte*. But because the magistrate judge's thoughtful opinion addressed a novel question on the scope of the Fifth Amendment's privilege against self-incrimination, the Court invited the Federal Defender Program in this District to file an *amicus* brief to defend the decision (the government did not object to the *amicus* participation). The Court is grateful for the Federal Defender Program's excellent service in fulfilling this request.[1] After reviewing the competing filings and the governing case law, the Court holds that requiring the application of the fingerprints to the sensor does not run afoul of the

[1] The Federal Defender Program in this District is led by Ms. Carol Brook, and the authors of the *amicus* brief are Program Attorneys Beth Jantz and Daniel McLaughlin.

self-incrimination privilege because that act does not qualify as a testimonial communication.

I.

In the search-warrant application, the government seeks authority to search a home for evidence of the possession and receipt of child pornography. The affidavit in support of the application spells out the facts that justify believing that at least one Apple iPhone and iPad will be found at the home. The magistrate judge found that the application established probable cause to search the home, as well as to seize electronic storage media (like computers, smartphones, and iPads) that could be used to store child pornography. R. 1 at 1. That probable-cause finding is not at issue in this review, and indeed the Court agrees with the finding. The magistrate judge also implicitly found that, because there are only four residents at the home, there is probable cause to believe that a device found there would belong to one of those residents, especially if that person is present during the search when the device is found. *See* R. 1 at 2. That probable-cause finding too is not at issue in this review.[2]

Going beyond the seizure of the devices, however, the government also asks for authorization to seize, in effect, the four residents in order to apply their fingers (including thumbs) to Apple-made devices (here, most likely iPhones and iPads)

[2]To be sure, in other situations the number of residents in a home could be so great that there would not be probable cause to believe that every resident could be the device's owner or have access to the device. But here the probable-cause finding is sound because there are only four residents, and the probable-cause standard itself is not a preponderance standard. *Cf. Maryland v. Pringle*, 540 U.S. 366, 371-72 (2003) (probable cause to believe all three occupants of car possessed drugs where drugs were found behind back armrest and bundle of cash was found in glove compartment).

found at the home. Affidavit ¶ 41. What animates this request is that the government does not know, of course, what the passcodes are to unlock any Apple devices found at the home. Affidavit ¶ 38. Data on Apple devices are likely encrypted, so without some way to unlock the device, the government will not be able to access and search it. Affidavit ¶ 38. But some iPhone and iPad models allow users to unlock the device by using a fingerprint instead of entering a passcode. Affidavit ¶ 35. Users can register up to five fingerprints for this unlocking feature, known as (on Apple devices) Touch ID. Affidavit ¶ 36. When a registered fingerprint is pressed against a sensor on the device, the device unlocks. Affidavit ¶ 36.

But there's a time-urgency with trying Touch ID to unlock a device. If more than 48 hours have passed since the last time the device was unlocked, Touch ID will not work—the passcode must be entered. Affidavit ¶ 37. If a user remotely locks the device, Touch ID will not work. *Id.* If a device has been turned off or restarted, Touch ID will not work. *Id.* So to take advantage of this potential way of unlocking an iPhone or iPad, the government asks that the four residents of the home—if they are present during the search—be required to press fingers, chosen by the government, to the Touch ID sensor:

> … I request that the Court authorize law enforcement to press the fingers (including thumbs) of [the four residents] 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.

Affidavit ¶ 41. There is a practical limitation on the number of fingers that the agents can try, because Touch ID will not unlock the device after five failed attempts to use Touch ID—after that, the passcode must be entered. Affidavit ¶ 37.

As noted earlier, the magistrate judge denied authorization for the fingerprint seizure, holding that the compelled pressing of the fingerprint against the Touch ID sensor would violate the Fifth Amendment's privilege against self-incrimination. The magistrate judge reasoned that providing the fingerprint under these circumstances was akin to implicitly communicating that the device was within that person's possession and control. R. 1 at 17-18. After the denial of the fingerprint-seizure authority, the government sought review under Local Criminal Rule 50.4(a).[3]

II.

The privacy concerns at stake in government access to smart devices are intense, both because of the nature of the information that people store on those devices—pretty much every kind of information there is, from personal, financial, and professional—and because of the sheer volume of information that can be stored on them. But the constitutional text, as interpreted by governing case law, draws a distinction between compelling a person to *communicate* something to the government versus compelling a person to provide some *physical* characteristic as part of an investigation. Indeed, as the Supreme Court has explained, this

[3] During the review of the warrant application, the Court required the government to submit an updated affidavit for purposes of ensuring that the probable cause was not stale. The updated affidavit has been made part of the record (under seal for now), and the citations in this Opinion are to the updated version of the affidavit.

distinction renders what is widely known as the "privilege against self-incrimination" as something of a misnomer. *United States v. Hubbell*, 530 U.S. 27, 34 (2000) ("[t]he term 'privilege against self-incrimination' is not an entirely accurate description of a person's constitutional protection").

Specifically, the constitutional text on which the right is premised only prevents the government from compelling a person from being a "witness" against himself. U.S. Const., amend. V. The Fifth Amendment provides, in pertinent part: "No person … shall be compelled in any criminal case to be a *witness* against himself." *Id.* (emphasis added). Witnesses provide *testimony*, so that specifically is the forbidden compulsion: the government cannot force someone to provide a communication that is "testimonial" in character. *Hubbell*, 530 U.S. at 34. With that limit in mind, the Supreme Court has distinguished between compelling a communication versus compelling a person to do something that, in turn, displays a physical characteristic that might be incriminating. *Id.* at 35. For examples, the Supreme Court has held that compelling displays of the following physical features do not violate the privilege against self-incrimination:

- Putting on a shirt to see whether it fit the defendant. *Holt v. United States*, 218 U.S. 245, 252-53 (1910).
- Providing a blood sample to test for alcohol content. *Schmerber v. California*, 384 U.S. 757, 763-65 (1966).
- Submitting to the taking of fingerprints or photographs. *See Schmerber*, 384 U.S. at 764; *United States v. Wade*, 388 U.S. 218, 223 (1967).

- Providing a voice exemplar, that is, being compelled to say certain words spoken by a suspect so that the victims of a bank robbery could compare the defendant's voice to that of the bank robber. *United States v. Wade*, 388 U.S. 218, 222-23 (1967).

- Providing a handwriting exemplar, that is, being compelled to write words in order to compare them with the writing on a bank-robbery demand note. *Gilbert v. California*, 388 U.S. 263, 266-67 (1967).

The items on this list have a common thread: each of the compelled acts provided a physical characteristic of some sort, and nothing that the person did in performing the act *itself* comprised a communication by that person. There is no communicative expression by a suspect in putting on a shirt, giving a blood sample, having a fingerprint or photograph taken, or providing a voice or handwriting sample. To be sure, some of the compelled acts *could* have—and indeed, ordinarily *do* have—a communicative aspect when not performed in compliance with a law-enforcement directive. Some shirts have messages, people convey their moods and express ideas about themselves in photographs, and of course speaking and writing are fundamental forms of communication. But when a person does those things in compliance with an order to do so, we understand that the person is only providing a physical characteristic, not expressing themselves.

The same holds true for the fingerprint seizure sought by the government here. As noted earlier, and worth emphasizing again, the government agents will pick the fingers to be pressed on the Touch ID sensor, Affidavit ¶ 39 n.9, ¶ 41, so there is no need to engage the thought process of any of the residents at all in effectuating the seizure. The application of the fingerprint to the sensor is simply the seizure of a physical characteristic, and the fingerprint by *itself* does not

communicate anything. This reasoning has been applied by the very few cases that so far have addressed the issue. *State v. Diamond*, 890 N.W.2d 143, 150-51 (Minn. Ct. App. 2017), *review granted*, Case No. A15-2075 (Minn. Mar. 28, 2017); *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

Against this conclusion, the amicus argues that the magistrate judge correctly likened the fingerprint seizure to the communication that is inherent in the act of producing documents in response to a broad grand jury subpoena. In *United States v. Hubbell*, the defendant was served with a subpoena that sought 11 categories of documents. 530 U.S. 27, 31 (2000). After the defendant gathered responsive records, he ended up producing 13,120 pages of documents. *Id.* Following a line of precedent, the Supreme Court held that the defendant had been compelled to implicitly communicate facts via the act of production: specifically, that the records existed, were in his possession or control, and were authentic, as well as that the document production was a complete response to the subpoena. *Id.* at 37-38. (citing *United States v. Doe*, 465 U.S. 605, 614 (1984); *Fisher v. United States*, 425 U.S. 391, 409-10 (1976)).

But this act-of-production line of cases is distinguishable. In *Hubbell*, the very act of production *itself* implied what was in the subpoena recipient's mind:

> Given the breadth of the description of the 11 categories of documents called for by the subpoena, the collection and production of the materials demanded was tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions.

Id. at 41. In order to answer the subpoena, the defendant had to make "extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena." *Id.* at 43 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957) and citing *Doe*, 487 U.S. at 210). So the act of producing the records *inherently* represented communications from the defendant.

Not so with the fingerprint seizure. The government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without need for the person to put any thought at all into the seizure. The amicus's position would be correct if the warrant required the *person* to decide which finger (or fingers) to apply. But when agents pick, the person's performance of the compelled act is not an act of communication by that person. Indeed, the person can be asleep—and thus by definition not communicating anything—when a seizure of this sort is effectuated. If anything, handwriting and voice exemplars require a person to engage more mental processes than simply providing a finger for application to the Touch ID sensor. And if anything, handwriting and voice exemplars contain more implicit admissions than a fingerprint, namely, that 'I can write and this is my handwriting,' or 'this is my voice and this is how I pronounce this word.' *See Fisher*, 425 U.S. at 411 ("When an accused is required to submit a handwriting exemplar he admits his ability to write and impliedly asserts that the exemplar is his writing.").[4]

[4] Tattoos are another physical characteristic that arguably have more of a communicative aspect than fingerprints seizures, and yet the display of tattoos has been held to be a display of physical characteristics and not a testimonial communication. *People v. Slavin*, 807 N.E.2d 259, 263-64 (N.Y. 2004).

In contrast, the fingerprint seizure is just that—the agents seize a finger and apply it to the sensor, and that act does not make use of the content of the person's mind.

The amicus and the magistrate judge characterize the fingerprint seizure as containing an implicit communication when the fingerprint is *applied* to the Touch ID sensor: if the device unlocks, then the incriminating inference is that the person had possession or control of the device. But the government correctly responds that the fact that the physical characteristic yields incriminating information is *not* the dividing line between whether a compelled act comprises testimonial communication or not. The Supreme Court made this point in *Doe*, when approving a court order that compelled a person to sign a generic consent form to obtain bank account records. 487 U.S. at 215-16. In *Doe*, the generic consent form did not identify any specific bank or bank account, so the person's signing of the form would not convey any particular piece of information. *Id.* at 215. The Supreme Court rejected the argument that the consent form was testimonial merely because the government could *use* the form to advance its investigation. *Id.* at 208-09. That argument, the Court explained, conflated the inquiry of whether the compelled signing was "testimonial" with the inquiry of whether it would be incriminating. *Id.* at 209-10. If a compelled act is not testimonial, then the privilege against self-incrimination does not apply—even if the act is incriminating. *Id.* at 210 ("the Court has held that certain acts, *though incriminating*, are not within the privilege") (emphasis added).

That distinction—between whether an act is testimonial versus whether the act is incriminating—explains why physical characteristics, like fingerprints, blood samples, handwriting, and so on are not protected by the privilege even though they often are highly incriminating. When deciding whether an act is testimonial or not, the governing case law simply does not take into account the power or immediacy of the incriminating inference acquired from the physical characteristic. If the act does not *inherently* contain a communication from the person, then no testimony has been obtained from the person. In essence, applying the fingerprint to the Touch ID sensor is no different than watching someone put on a shirt to see—immediately—if it fits or listening to someone speak in a live lineup and deciding—immediately—whether the voice matches the suspect's. And the speed, or relative lack of speed, in obtaining the results is not a dividing line, even as fingerprint and blood-sample analyses have sped up in recent years. The fingerprint seizure itself contains no communication, just as those other physical characteristics do not themselves communicate anything.

The amicus also offers another basis to distinguish the fingerprint seizure from other physical characteristics: unless unlocked via the Touch Sensor or via a passcode, the contents of the iPhone or iPad would otherwise be encrypted and undecipherable to the government. So, the argument goes, the fingerprint seizure has a communicative aspect because it decrypts the data into an accessible form, thus providing information to the government. But this argument too relies on conflating what it means for an act to be inherently testimonial versus an act

yielding an incriminating result. Again, the fingerprint seizure itself does not reveal the contents of the person's mind in the way that disclosure of a passcode would or in the way that disclosure of a cryptography key would. Yes, compelling someone to reveal information on how to decrypt data is compelling testimony from that person. But obtaining information from a person's mind is not what happens when agents pick a finger to apply to the sensor. So compelling physical access to information via the fingerprint seizure is no different from requiring someone to surrender a key to a safe whose contents otherwise would not be accessible to the government. The surrender of the key may be compelled, but the compelling of the safe's combination is forbidden. *See Doe*, 487 U.S. at 210 n.9 (signing generic consent form does not force a person "to express the contents of his mind," so it is more like surrendering a key rather than revealing the combination"). The same principle applies here: a person generally cannot be compelled to disclose the passcode (like the safe's combination) but can be compelled to provide the fingerprint (like the key to the safe).

The thought-provoking decryption argument advanced by the amicus does raise, again, the intensity of the privacy interests at stake in accessing smart devices. As the amicus and the magistrate judge both observed, the Supreme Court has recognized the "vast quantities of personal information" stored on those devices, raising the prospect of extensive intrusion due to both the quantity and nature of the accessed information. *Riley v. California*, 134 S. Ct. 2473, 2485, 2490 (2014). Indeed, in some ways the information at stake goes beyond even what is usually

stored in that most private of places—the home. *Id.* at 2491. *Riley* teaches the need for courts to be sensitive to how the digital age might alter legal principles.

But it is one thing to describe *Riley*'s lesson at that high level of generality, and quite another to apply the lesson to concrete legal decision-making. Remember that, in *Riley*, the Supreme Court interpreted the Fourth Amendment, which prohibits "unreasonable" searches and seizures. U.S. Const., amend IV. By necessity, interpreting a term like "unreasonable" has required the Supreme Court to engage in the balancing of interests, government versus private. And that is what the Court did in *Riley*, assessing the various governmental interests (such as officer safety and preventing the destruction of evidence) versus the privacy interests of individuals in the contents of their smartphones. 134 S. Ct. at 2484 (describing "balancing of interests" underlying the search incident to arrest exception); *id.* at 2485-91. After balancing those interests, the Court held that the Fourth Amendment requires that the government obtain a search warrant before searching a smartphone. *Id.* at 2495.

Here, however, the interpretive task is to decide whether the fingerprint seizure amounts to requiring a person to be a "witness" against himself or herself, as barred by the Fifth Amendment. U.S. Const., amend V. That is a different exercise in interpretation from the balancing test necessitated by the word "unreasonable" in the Fourth Amendment. The word "witness" still limits the scope of the privilege against self-incrimination to those acts that are themselves *testimonial* in nature, regardless of how the digital age has raised the stakes on the

amount and type of information that might result from the compelled, non-testimonial act. So, although *Riley* certainly instructs courts to avoid mechanical application of legal principles in the face of technological advances, the constitutional text dictates the result here.

III.

For the reasons discussed, the government's application to require the fingerprint seizure of the four residents does not violate the privilege against self-incrimination set forth in the Fifth Amendment. The question is close enough that the Court has suggested that the government consider assigning a "screen" team to review the contents of devices accessed with the fingerprint seizure, out of both fairness to the residents and to guard against an argument that, if this Opinion is wrong, then the entire remainder of the investigation was tainted by the information obtained via the fingerprint seizure.

Finally, it is worth noting that this decision does not address whether the Fourth Amendment would permit the government to obtain a fingerprint seizure, like the one in the warrant, via a grand jury subpoena. Nor does this decision reflect a comment, one way or the other, on whether there ought to be regulation of this investigative tactic beyond what is dictated by the Constitution. In light of the policy interests at stake, perhaps Congress will study whether there ought to be statutory limits; the legislature is better positioned to balance the interests of law enforcement and privacy interests, as it has in calibrating, for example, the governmental interests in relation to the severity of the crime under investigation.

See 18 U.S.C. 3142(f)(1) (providing for presumption of detention based on the severity of the alleged crime).

This Opinion will be entered under seal for now, in light of the ongoing investigation and contemporaneous execution of the search warrant. After the execution of the search warrant, at a later appropriate time when there is no risk either to the investigation or to publicly (and unfairly) inferring the identity of the residents, the Court will unseal a redacted version of this Opinion and of the briefs. The Court will confer with the government and the amicus before doing so.

ENTERED:

s/Edmond E. Chang
Honorable Edmond E. Chang
United States District Judge

DATE: September 18, 2017