IN THE CIRCUIT COURT OF COOK COUNTY
SECOND MUNICIPAL DISTRICT – SKOKIE, ILLINOIS

In the Matter of the Search	)	
Of One White iPhone X Cellular	)	No. [redacted]
Telephone in the Custody of the	)	Hon. Paul S. Pavlus
Niles Police Department	)	

MEMORANDUM OF LAW IN SUPPORT OF RESPONDENT [redacted] MOTION TO RECONSIDER

Respondent [redacted], by and through his attorneys, submits this memorandum of law in support of his motion to reconsider this Court's order compelling Respondent "to provide the passcode to his White iPhone X to the Niles Police Department in order to comply with search warrant [redacted]."

Introduction

Respondent [redacted] objects to the Court's order of January 18, 2019, compelling Respondent to provide the passcode to his phone, as the order is not authorized under Illinois law. It also violates the Fifth and Fourteenth Amendments of the United States Constitution, as well as the Illinois state constitution.

As an initial matter, Illinois courts lack jurisdiction to order the target of a search warrant to assist in executing that warrant or explaining any items that the State may find. But that is precisely what Respondent [redacted] has been commanded to do here. There is no provision in Illinois law that authorizes courts to issue device decryption orders, like the one this Court entered on January 18, 2019. Rather, the absence of any positive law on point indicates the legislature's healthy respect for the

basic constitutional right against self-incrimination. The compelled decryption order here is *ultra vires* and categorically impermissible under Illinois law.

Second, even if, assuming *arguendo*, Illinois courts had the statutory authority to issue decryption orders generally, the order here violates Respondent [redacted]'s federal and state constitutional rights against self-incrimination. *See* U.S. CONST. amend V; ILL. CONST. art. I, § 10. The act of unlocking and decrypting the White iPhone X would be compelled, testimonial, and potentially incriminating. Furthermore, the "foregone conclusion" doctrine does not apply here, as the State cannot show with reasonable particularity that the information it would obtain from unlocking and decrypting the iPhone is already known to the State. As a result, Respondent [redacted] is entitled to assert his constitutional rights and refuse to assist law enforcement in their efforts to discover evidence to use against him in a criminal case.

Relevant Facts

The Niles Police Department is investigating a fatal accident that occurred on December 27, 2018. As part of that investigation, officers from the Niles Police Department detained Respondent [redacted] on the evening of December 27, 2018, during which time officers physically seized a White iPhone X. The Niles Police Department eventually released [redacted] from custody, pending further investigation, without pressing any charges or issuing any traffic citations. Nonetheless, the Department sought and obtained a search warrant signed by Judge Lauren Gottainer Edidin on December 28, 2018, authorizing the search of [redacted]'s

iPhone. Separately, on January 18, 2019, this Court ordered [redacted] "to provide the passcode to his White iPhone X to the Niles Police Department in order to comply with [the] search warrant." *See* Exhibit 1, 12-28-2018 Search Warrant; Exhibit 2, 01-18-2019 Court Order Compelling Respondent to Provide Passcode ("Decryption Order"). Respondent, with the undersigned, appeared in court on January 21, 2019 (the first business day after the Court's January 18, 2019 order), formally objecting to the compelled decryption order. He now files this Memorandum of Law in support of his Written Objection and Motion to Reconsider the *Ex Parte* Compelled Decryption Order.

Argument

Respondent [redacted] opposes the order commanding him to provide the passcode to the White iPhone for two reasons. First, state law does not authorize Illinois courts to order the target of a search warrant to assist officers in executing it. Second, such an order would violate [redacted]'s federal and state constitutional rights against self-incrimination. *See* U.S. CONST. amend V; ILL. CONST. art. I, § 10; *People v. McCauley*, 163 Ill. 2d 414, 452, 645 N.E.2d 923, 942 (1994) (noting that the federal and state privileges are coextensive).

I. Illinois Law Does Not Authorize Courts to Issue Compelled Decryption Orders

The Decryption Order issued by this Court cites no legal authority to compel Respondent [redacted] to unlock and decrypt the White iPhone X. That is because there is no Illinois law authorizing courts to issue such orders in aid of search warrants, *see*

725 ILCS 5/108-1 *et seq.*, and there is no authority from the Illinois Supreme Court sanctioning such orders.

To be sure, the Illinois state legislature does authorize state courts to compel the production of evidence in certain circumstances, but this is not one of them. For instance, the legislature has vested broad power in grand juries to compel the production of documents. 725 ILCS 5/112-4; *see also In re May 1991 Will Cty. Grand Jury*, 152 Ill. 2d 381, 389, 604 N.E.2d 929, 933 (1992). Likewise, the legislature has crafted a process for subpoenas duces tecum for investigations involving the sexual exploitation of children, 725 ILCS 5/115-17b. The legislature, of course, also allows the issuance of a subpoena to produce physical evidence at trial. 725 ILCS 5/115-17.

Nothing in the rules of Illinois criminal procedure, however, grants courts the power to compel the target of a search warrant to unlock and decrypt a digital device. Given the detailed rules for other forms of compelled production, the absence of any statute on point indicates that the legislature did not intend to vest courts with this authority. *See People v. McCarty*, 223 Ill. 2d 109, 125, 858 N.E.2d 15, 26 (2006) ("In the absence of the legislature's express statement of such a limitation, we decline to read one into the statute.")

It is not surprising that the Illinois legislature has declined to authorize such compulsion orders in support of search warrants. Doing so would violate basic constitutional prohibitions against self-incrimination, as discussed in section II. Federal Courts have the general authority to compel the production of evidence "in aid of their respective jurisdictions" under the All Writs Act, 28 U.S.C.A. § 1651 (West

2019), but no similar provision exists in the Illinois Constitution, or the Illinois Code of Criminal Procedure.

Even if this Court were to construe the Decryption Order as a subpoena duces tecum, which it is not, any analogy to the production of physical documents would miss the mark. As the Supreme Court has repeatedly emphasized, courts are not to analogize iPhones to filing cabinets and paper documents. *See Riley v. California*, 134 S.Ct. 2473, 2491, 2495 (2014) (cell phones "hold for many Americans the 'privacies of life,'" a search of which "would typically expose to the government far more than the most exhaustive search of a house"); *Carpenter v. United States*, 138 S.Ct. 2206, 2222 (2018) (finding that cell phone location data is "an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers"). In short, digital devices are different from other storage devices and should be treated differently. *In re Search of Residence in Oakland, California*, No. 4-19-70053, 2019 WL 176937, at *4 (N.D. Cal. Jan. 10, 2019) ("mobile phones are subject to different treatment than more traditional storage devices, such as safes, and should be afforded more protection"). Consequently, there is no statutory authority for this Court to order Respondent [redacted] to unlock and decrypt the White iPhone X.

II. Compelled Decryption Orders Violate Federal and State Constitutional Rights Against Self-Incrimination

The Fifth Amendment to the United States Constitution provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S.

CONST. amend. V. The Illinois State Constitution contains a nearly identical guarantee. ILL. CONST. art. I, § 10 ("No person shall be compelled in a criminal case to give evidence against himself.").

The Fifth Amendment applies when the government seeks to (1) *compel* an individual to provide (2) a *testimonial* communication or act that is (3) *incriminating*. *See Fisher v. United States*, 425 U.S. 391, 409 (1976). Here, there should be no dispute that the State seeks to compel Respondent [redacted] to unlock and decrypt the iPhone by forcing him to provide the Niles Police Department with the passcode. Likewise, it is clear the State believes that access to the unencrypted phone data will yield incriminating evidence against Respondent [redacted]. The critical question is whether providing the passcode and decrypting the data is "testimonial" under the Fifth Amendment.

Requiring Respondent to unlock and decrypt his iPhone is inherently testimonial. It is no mere physical act. Rather, like providing the combination to a safe, it requires him to use the contents of his mind to aid in the State's investigation. Additionally, the decryption process uses the passcode to translate otherwise unintelligible data into a form that can be used and understood by the State, effectively requiring Respondent [redacted] to not only unlock the safe, but also explain the meaning of the items discovered inside.

A. The State Seeks to Compel Respondent to Divulge the Passcode

There is no serious dispute that Niles Police Department is attempting to compel Respondent [redacted] to provide the passcode to the White iPhone X seized

on December 28, 2018. *In re Marriage of Roney*, 332 Ill.App.3d 824, 827 (4th Dist. 2002) (husband was "compelled" to turn over evidence because the trial court ordered him to produce recordings and, when he did not, held him in contempt).

B. Providing a Passcode Is "Testimonial"

The State seeks to compel Respondent [redacted] to "provide" the passcode to the White iPhone X. Decryption Order at 1. The Order does not specify whether [redacted] must input the code directly into the device or disclose it in some other way to the Niles Police Department. But in any event, the Order seeks "testimonial" communications under the Fifth Amendment because it would require [redacted] to reveal "the contents of his own mind" to comply. *Hubbell*, 530 U.S. at 29.

The privilege against self-incrimination protects against compelled "testimonial" communications, verbal or otherwise. *Doe v. United States* ("*Doe II*"), 487 U.S. 201, 210 n.9 (1988) (agreeing on this point with Stevens, J., dissenting, *id*. at 219). The focus is not on whether the communication is spoken, but whether it involves, by "word or deed," an "expression of the contents of an individual's mind." *Id*. at 219, 220 n.9 (Stevens, J., dissenting).

Thus, as the Supreme Court has explained, compelling the production of the combination to a wall safe is testimonial, whereas requiring the surrender of a key to a strongbox is not. *Id*. at 220. The first reveals the contents of one's mind; the second is a "simple physical act." *United States v. Hubbell*, 530 U.S. 27, 29 (2000). Other such "mere physical act[s]," *id*. at 43, include: wearing a particular shirt, *Holt v. United States*, 218 U.S. 245, 252–53 (1910), providing a blood sample, *Schmerber v.*

California, 384 U.S. 757, 761 (1966), providing a handwriting exemplar, *Gilbert v. California*, 388 U.S. 263, 266–67 (1967), and producing certain known business documents, *Fisher v. United States*, 425 U.S. 391, 412–13 (1976).

By contrast, providing the passcode to unlock and decrypt an iPhone requires expressing the contents of one's mind. *See United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quashing a subpoena for computer passwords, reasoning that, under *Hubbell* and *Doe*, the subpoena would have required the suspect "to divulge through his mental process his password"); *G.A.Q.L. v. State*, 257 So. 3d 1058 (Fla. Dist. Ct. App. 2018) (passcodes of minor's cellphone, which were sought by police following a vehicle accident in which the passenger was killed, were testimonial in nature and implicated the Fifth Amendment protections against self-incrimination); *Comm. v. Baust*, 89 Va. Cir. 267 (2014) ("compelling Defendant to provide access through his passcode is both compelled and testimonial, and, therefore, protected"); *Comm. v. Jones*, No. 2017CR49, 2017 WL 3340408, at *4 (Mass. Super. July 26, 2017); *In re Search of a Residence in Oakland, California*, No. 4-19-70053, 2019 WL 176937 at **3-4 (N.D. Cal. Jan. 10, 2019); *In re Application for a Search Warrant*, 236 F.Supp.3d 1066, 1073-74 (N.D. Ill. 2017); *see also In re Marriage of Roney*, 332 Ill.App.3d at 827-28 (holding that production of surreptitious audio recordings would violate the Fifth Amendment privilege).

Just like a computer password or safe combination, compelling Respondent [redacted] to enter the numeric passcode for the iPhone would be testimonial. *See Hubbell*, 530 U.S. at 43; *Kirschner*, 823 F. Supp. 2d at 669. All of these physical acts

require remembering, recalling, and inputting information that exists nowhere but in the mind. Consequently, compelling the passcode is testimonial for Fifth Amendment purposes. Nothing more is necessary to implicate the privilege.

i. Modern iPhone Features Make Compelled Decryption Inherently Testimonial

Compelled decryption is inherently testimonial, not only because it forces a person to reveal the contents of their mind to the State, but also because it involves translating otherwise unintelligible evidence into a form that can be used and understood by the State.

Like all modern iPhones, the iPhone in this case is not merely locked, but also encrypted. That means its data is automatically kept in a scrambled, unintelligible format, like a secret code. Only those who possess the decryption "key" can transform this scrambled data back into meaningful information. And as a result, anyone who simply breaks into an encrypted device will not be able to "read" the data stored on it – unless they have the key necessary for decoding the information back into its unscrambled and intelligible state.

On modern iPhones, encryption keys are inextricably linked with the passcodes users set to lock and unlock their devices. Technically speaking, a passcode "provides entropy for certain encryption keys," meaning that, in addition to unlocking the device, it is a foundational part of the encryption and decryption process.[1] As a result, the "stronger the user passcode is, the stronger the encryption key becomes."

[1] Apple, Inc., iOS Security (Nov. 2018) at 18, *available at* https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf (last visited February 3, 2019).

Id. In other words, the passcode is not merely the combination to a wall safe – it is also a big part of the secret "key" necessary to decode (unencrypt) the information it contains.[2]

Thus, although compelling the production of a passcode is significantly similar to compelling the combination to wall safe, it is also an imperfect analogy.[3] It does not tell the whole tale of how the technology works or account for the vital role it plays in decrypting user data.

The combination to a vault might provide access to preexisting documents, but it would not normally provide the State with a key to understanding them. By contrast, entering the passcode to an iPhone not only unlocks the device, but also transforms any preexisting, scrambled data into intelligible content. It communicates the content and characteristics of each and every file within the encrypted space. *See Hubbell*, 530 U.S. at 43. Indeed, it communicates whether any files exist at all. *See id*. ("[W]e have no doubt that the constitutional privilege against self-incrimination protects . . . from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence.").

Here, the State seeks not merely the surrender of inaccessible documents, as in the case of a safe, but also the transformation and translation of whatever

---

[2] *See generally* David G. Ries & John W. Simek, *Encryption Made Simple For Lawyers*, 29 GPSolo 6 (Dec. 2012), *available at* https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers (last visited February 3, 2019).

[3] *See, e.g.,* Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. PUB. INT. L.J. 53, 77 (2015).

information may be inside. It is akin to compelling the subject of a search warrant to not only provide the combination to the safe, but also then explain the meaning of any items or documents discovered.

In fact, the Niles Police Department is currently in possession of every bit of data sought in the December 28, 2018 search warrant issued by Judge Edidin. Investigators simply cannot make sense of it. In this light, they possess the pieces of an extremely complex jigsaw puzzle that they are unable to complete. This Court's January 18 order, compelling Respondent [redacted] to provide the passcode, is like making him use his unique knowledge to assemble that puzzle for the purpose of aiding in his own prosecution.

In sum, compelled, passcode-based decryption requires using the contents of one's mind to not just "unlock" the device, but also to translate and explain the seized data to the government. It is inherently testimonial and, therefore, always protected by the Fifth Amendment privilege against self-incrimination.

ii. Prohibiting Compelled Decryption Furthers the Values Animating the Fifth Amendment Privilege Against Self-Incrimination

As the Supreme Court has explained, the privilege against self-incrimination has its roots in the nation's historical "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury, or contempt[,]" out of "respect for the inviolability of the human personality and the right of each individual to a private enclave where he may lead a private life." *Doe II*, 487 U.S. at 212-13 (quoting *Murphy v. Waterfront Comm'n of New York Harbor*, 378 U.S. 52, 55 (1964)) (internal

quotations omitted). The privilege against self-incrimination "enables the citizen to create a zone of privacy which the government may not force him to surrender to his detriment." *In re Grand Jury Proceedings*, 632 F.2d 1033, 1043 (3d Cir. 1980). It represents the judgment of the Founding Fathers that, "in a free society, based on respect for the individual, the determination of guilt or innocence by just procedures, in which the accused made no unwilling contribution to his conviction, was more important than punishing the guilty." *Id.* (internal quotations omitted). And above all, it ensures "the right of each individual to a private enclave where he may lead a private life," free from wholesale inspection by government agents. *Doe II*, 487 U.S. at 212 (internal quotations omitted).

In an age when cell phones "hold for many Americans 'the privacies of life,'" *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014), courts must take care to ensure that rapid advances in technology do not erode this basic American right. *See Carpenter v. United States*, 138 U.S. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S., 27, 34 (2001) (the Court has repeatedly sought to "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.") (internal quotations omitted)). "Citizens do not contemplate waiving their civil rights when using new technology, and the Supreme Court has concluded that, to find otherwise, would leave individuals 'at the mercy of advancing technology.'" *In re Search of Residence in Oakland, California*, No. 4-19-70053, 2019 WL 176937, at *2 (N.D. Cal. Jan. 10, 2019) (citing *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 35)).

C. Compelled Decryption is Potentially Incriminating

Whether compelled decryption of the iPhone is incriminating rests on whether the act will lead to the discovery of incriminating evidence. *Hubbell*, 530 U.S. at 37. This test applies to testimonial acts that "would in themselves support a conviction ... but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant." *Hoffman v. United States*, 341 U.S. 479, 486 (1951).

Here, the Niles Police Department obtained a search warrant for Respondent [redacted]'s iPhone, averring probable cause that five categories of data on the phone "have been used in the commission of," "constitute evidence of," or "constitute the fruits of the offense of" aggravated DUI and reckless homicide. Assuming *arguendo* that such information exists on the phone, compelling [redacted] to unlock the phone and decrypt that data would lead to the discovery of incriminating evidence. It would also convey to the State that he exercises control over the phone, has knowledge of and access to its contents, and could serve to authenticate the data it contains.

The only reason the State seeks to compel Respondent [redacted] to unlock and decrypt the phone is that the State believes the phone contains data that will incriminate [redacted]. If that is not true, then there is no basis for a search of the phone in the first place. But assuming there is sufficient probable cause to support the search warrant,[4] then forcing Respondent [redacted] to unlock and decrypt the

[4] Respondent does not concede there existed probable cause for the issuance of the search warrant signed on December 28, 2018, as Respondent has not yet been able to examine the affidavit submitted in support of issuance of the search warrant.

White iPhone X would likely lead to the discovery of incriminating evidence against him. It is abundantly clear that compelling [redacted] to unlock and decrypt the iPhone is the first step in providing the State with a "lead to incriminating evidence" or "a link in the chain of evidence needed to prosecute." *Hubbell*, 530 U.S. at 38 (citing *Hoffman*, 341 U.S. at 286, and *Doe II*, 487 U.S. at 208 n.6).

D. The "Foregone Conclusion" Doctrine Does Not Apply

Even if compelled decryption is not inherently testimonial, the act of production in this case still violates the Fifth Amendment because the nature of the information communicated to the State is not a "foregone conclusion."

The "foregone conclusion" doctrine holds that the act of producing documents has no testimonial value when the State can show with "reasonable particularly" that it already knows the existence, location, and authenticity of the documents it seeks. *See Fisher*, 425 U.S. at 410-11; *Hubbell*, 530 U.S. at 45; *In Re Grand Jury Subpoena*, 670 F.3d at 1346. The doctrine applies only when the resulting production "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. That is a stringent burden, and the State cannot satisfy it by simply demonstrating its knowledge of the existence, location, and authenticity of the physical device. Instead, the State must make this showing with respect to the information it seeks. *SEC v. Huang*, No. 15-269, 2015 WL 5611644, at *2 (E.D. Pa. Sept. 23, 2015) (discussing *In re Grand Jury Subpoena*, 670 F.3d at 1346); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1063 (Fla. Dist. Ct. App. 2018) ("It is critical to note here that when it comes

to data locked behind a passcode wall, the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall.").

The government could not meet this burden in *Hubbell*, 530 U.S. at 44-45, because it had no "prior knowledge of either the existence or the whereabouts" of the 13,120 pages produced by the suspect in response to a subpoena. And it could not overcome its failure of proof by arguing that business people "always possess general business and tax records that fall within the broad categories described in the subpoena." *Id*. at 45. On the other hand, the government met its burden in *Fisher* when it sought specific financial records from taxpayers that had been prepared by accountants and provided by the taxpayers to their attorneys in connection with an IRS investigation. 425 U.S. at 394. The government knew that the documents were in the attorneys' possession and it could independently confirm their existence and authenticity through the accountants who created them. *See id*. at 411 (noting that the records in question "belong[ed] to the accountant" and "were prepared by him"). Under these circumstances, "[t]he existence and location of the papers [we]re 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*.

Here, the act of unlocking and decrypting the iPhone would constitute testimony about Respondent [redacted]'s "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." *In re Grand Jury Subpoena*, 670 F.3d at 1346. Yet the State cannot show that it knows

"whether any files exist and are located on the [device]"; whether [redacted] was "even capable of accessing the encrypted portions of the [device]"; and "whether there was data on the encrypted [device]." *Id.* at 1346-47. As the Eleventh Circuit emphasized, because encryption generates "random characters if there are files *and* if there is empty space," it is impossible to know what, if anything, is hidden on the device. *Id.* at 1347 (emphasis original). Thus, as in *Hubbell* and unlike *Fisher*, the State does not know "the existence or the whereabouts" of the information it seeks.

Further, where the State does not know "specific file names," it must show with "reasonable particularity" that it seeks "a certain file," and can establish that "(1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *Id.* at 1349 n.28. "[C]ategorical requests for documents the Government anticipates are likely to exist simply will not suffice." *Id.* at 1347. Thus, while requests describing a general category of documents may be sufficient for obtaining a search warrant, the Fifth Amendment demands something more.

State and federal courts throughout the country have reached similar conclusions. In *G.A.Q.L. v. State*, a Florida appellate court held that the foregone conclusion doctrine did not apply to compelled production of a cell phone passcode where the government "fail[ed] to identify any specific file locations or even name particular files that it seeks" from the encrypted device. 257 So. 3d at 1064 (Fla. Dist. Ct. App. 2018). The court emphasized that the focus of the inquiry is "not the verbal recitation of a passcode, but rather the documents, electronic or otherwise, hidden by

an electronic wall." *Id.* As a result, it is insufficient to simply show that Respondent knows the passcode to his own phone. A contrary holding would "expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment." *Id.* at 1063.

Similarly, in *Huang*, the Eastern District of Pennsylvania denied a motion to compel smartphone passwords because doing so would "require intrusion into the knowledge of Defendants" and because the SEC could not establish with "reasonable particularity" that any documents sought resided in the locked phones. 2015 WL 5611644, at **2-3. By contrast, in *In re Boucher*, No 06-91, 2009 WL 424718, **2-3 (D. Vt. Feb. 19, 2009), the court found the foregone conclusion test satisfied where the government had already viewed contents of the drive in question, knew the existence and location of the drive's files, and ascertained that the files may consist of images or videos of child pornography. And in *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235–37 (D. Colo. 2012), the court also found the foregone conclusion test satisfied where the defendant had admitted in a recorded phone call that incriminating information was on the laptop. In both *Boucher* and *Fricosu*— and unlike in either *Huang* or *In re Grand Jury Subpoena*—the government had specific evidence that the information to be disclosed via decryption was a foregone conclusion.

In this case, the State cannot establish with reasonable particularity that all of the information it seeks to expose by compelling Respondent [redacted] to unlock and decrypt the iPhone is a foregone conclusion – let alone any specific file. Indeed, there

is no evidence that the State knows with reasonable particularity that any specific files will be found on the phone. Suspicion that a person has committed an offense – even suspicion sufficient to establish probable cause – is not sufficient to satisfy the government's burden of proving with reasonable particularity "the existence [and] the whereabouts" of specific files on the iPhone. *See* 670 F.3d at 1347 (requests for documents "the Government anticipates are likely to exist simply will not suffice"). And neither reasonable suspicion nor probable cause is sufficient to satisfy the government's heightened burden when seeking to overcome Respondent [redacted]'s Fifth Amendment protection against self-incrimination. *See id*. at 1349, n. 28.

The State's case thus falls far short of the specific factual bases presented in *Boucher* and *Fricosu* for satisfying the foregone conclusion doctrine. *Boucher*, 2009 WL 424718, *2 (agent observed apparent child pornography); *Fricosu*, 841 F. Supp. 2d at 1235 (suspect admitted specific information "was on [his] laptop"). Rather, just as in *In re Grand Jury Subpoena*, *G.A.Q.L.*, and *Huang*, the government cannot establish that it knew with reasonable particularity "whether any files exist and are located" on the iPhone prior to compelling [redacted] to decrypt the device. *See In re Grand Jury Subpoena*, 670 F.3d at 1346–47. Without reasonable particularity as to the encrypted files sought, the facts of this case "plainly fall outside" of the foregone conclusion doctrine. *Hubbell*, 530 U.S. at 44.

Conclusion

For these reasons, Respondent [redacted] respectfully moves this Honorable Court to reconsider its previous *ex parte* order and enter an order sustaining his written objection to the order.

Respectfully submitted,

By: /s/ Jonathan M. Brayman (47860)

Thomas M. Breen
Todd S. Pugh
Jonathan M. Brayman
Robert W. Stanley
BREEN & PUGH
53 West Jackson Boulevard
Suite 1215
Chicago, Illinois 60604
(312) 360-1001 (t)
(312) 362-9907 (f)
jbrayman@breenpughlaw.com

Attorneys for Respondent [redacted]

Michael Price
Senior Litigation Counsel
NACDL Fourth Amendment Center
1660 L Street NW, 12th Floor
Washington, DC 20036
(202) 465-7615
mprice@nacdl.org

Pro Bono Legal Research Assistance