ATTORNEYS FOR APPELLANT

William J. Webster
Carla V. Garino
Webster Legal, LLC
Westfield, Indiana

ATTORNEYS FOR APPELLEE

Curtis T. Hill, Jr.
Attorney General of Indiana

Ellen H. Meilaender
Supervising Deputy Attorney General
Indianapolis, Indiana

IN THE COURT OF APPEALS OF INDIANA

Katelin Eunjoo Seo,
Appellant-Defendant,

v.

State of Indiana,
Appellee-Plaintiff.

August 21, 2018

Court of Appeals Case No.
29A05-1710-CR-2466

Appeal from the Hamilton
Superior Court

The Honorable Steven R. Nation,
Judge

Trial Court Cause No.
29D01-1708-MC-5640

Mathias, Judge.

[1] Smartphones are ubiquitous in modern life. *See Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473, 2484 (2014) ("[M]odern cell phones, . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."). The

amount of personal information contained on a typical smartphone is astounding: photographs, contacts, emails, text messages, not to mention the personal information that is contained in widely used smartphone social-media applications such as Facebook, Instagram, LinkedIn, or Twitter. *United States v. Wurie*, 728 F.3d 1, 7 (1st Cir. 2013) (noting that "[I]nformation [contained on a modern cell phone] is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records."). Indeed, a modern smartphone is a "telephone" only as a small part of its many functions. It is more accurately described as a mobile computing and communications device with abilities that were dreams in the realm of science fiction only a few decades ago.

[2] Thus, when the State seeks to search a smartphone, it seeks to inquire into far more than "old-fashioned" information physically contained on paper. In truth, nearly every smartphone contains data stored and arranged in such a way as to uniquely reveal the innermost thoughts of its owner. A smartphone is a trove of extremely personal information that is almost always embarrassing, and potentially, incriminating. A modern smartphone, with its central purpose of connecting its owner to the Internet and its ability to store and share incredible amounts of information in "the Cloud" of online storage, is truly as close as modern technology allows us to come to a device that contains all of its owner's conscious thoughts, and many of his or her unconscious thoughts, as well. So, when the State seeks to compel a person to unlock a smartphone so that it may

search the phone without limitations, the privacy implications are enormous and, arguably, unique. *Cf. United States v. Otero,* 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs[.]").

[3] In the present case, the Hamilton Superior Court issued a search warrant ordering Katelin Eunjoo Seo ("Seo") not only to produce her smartphone,[1] but also to permit the State to search Seo's smartphone without limitation. Seo refused to unlock the phone, citing her right against self-incrimination under the Fifth Amendment to the Constitution of the United States ("Fifth Amendment," and "Constitution," respectively), and the State sought to hold her in contempt for her refusal to unlock the phone. The trial court agreed with the State and held Seo in contempt for refusing to unlock her phone. Seo appeals and argues that the trial court's order requiring her to unlock her phone violated the guarantee against self-incrimination contained in the Fifth Amendment. We agree. Accordingly, we reverse the trial court's order finding Seo in contempt and remand for proceedings consistent with this opinion, with

[1] The dissent claims that we "unnecessarily" hold that "a passcode is the equivalent of a combination to a wall safe," because the trial court did not ask Seo to reveal her password. Slip op., *infra*, at 55–56. The trial court's warrant and order, however, require Seo to unlock, and thereby decrypt, her phone. And the only way to unlock and decrypt the phone is for Seo to enter her passcode into the phone. As explained *infra*, we conclude that there is no meaningful difference between forcing Seo to reveal her passcode and forcing her to input her passcode into her phone and then handing it over to the police. Thus, we do not share the dissent's belief that our holding is unnecessary.

specific guidelines as to the reasonable specificity that prosecutors should show concerning the information sought in such an instance.

Facts and Procedural History

[4] In July 2017, Seo contacted the Hamilton County Sheriff's Department ("HCSD") claiming to be a victim of a rape committed by D.S. HCSD Detective Bill Inglis ("Detective Inglis") investigated Seo's allegations. As part of his investigation, Seo allowed Detective Inglis to view her smartphone, an Apple iPhone 7 Plus. With Seo's consent, Inglis also did a "forensic download" of the contents of Seo's iPhone and returned it to her. Tr. p. 6.

[5] After reviewing the contents of Seo's iPhone, Inglis decided not to pursue any charges against D.S. Instead, based on the contents of the phone and D.S.'s statements, Inglis began to investigate Seo for stalking and harassing D.S. When questioned, D.S. explained to Inglis that he received numerous calls and text messages from Seo's phone, up to thirty per day. At some point, however, the phone number of the sender of these messages and calls began to change daily, yet the conversations were linked and apparently sent by the same person. Inglis suspected that Seo was using a third-party application to change her phone number.[2]

[2] Detective Inglis mentioned two apps that could be used to change the caller's cellphone number: Google Voice and "Pinger," Tr. p. 8, the latter apparently a reference to the "Text Free Calling" app by Pinger, Inc., both of which are available for download on the Apple App Store for iPhones.

[6] On July 19, 2017, the State charged Seo with Level 6 felony stalking, Class A misdemeanor intimidation, Class A misdemeanor theft, and Class B misdemeanor harassment. The information alleged that Seo had stalked and harassed D.S. with the intent to get him to either marry her or impregnate her against his will. The police arrested Seo at her place of employment that same day. At the time of her arrest, Seo had in her possession a bag that contained an iPhone and an iPad tablet. Seo admitted that the phone was hers but claimed that the iPad belonged to someone else. The iPhone appeared to be the same one she had earlier provided to the police, and the number for the iPhone matched that of the phone used to make the earlier calls and send the text messages to D.S. The police took possession of Seo's iPhone at this time.

[7] On July 21, 2017, the State charged Seo under a new cause with thirteen counts of Class A misdemeanor invasion of privacy, alleging that Seo violated a protective order preventing her from contacting D.S. On August 8, 2017, the State applied for and was granted a warrant to search Seo's iPhone. Because Seo's iPhone is locked, the State also sought that same day a warrant and order compelling her to unlock her iPhone so that police could search it. The trial court issued a warrant providing in relevant part:

> WHEREAS, William Inglis of the Hamilton County Sheriff's Department has given sworn probable cause testimony for issuance of a Search Warrant. Based on that testimony, the Court finds probable cause exists for issuance of this Search Warrant.
>
> You are, therefore, authorized and ordered in the name of the State of Indiana, with necessary and proper assistance, in the

daytime or nighttime, to search the property located at and identified as:

5. for the purpose of searching items described in the sworn evidence, to wit:

> That Katelin Eunjoo Seo be compelled to unlock (via biometric fingerprint passcode, password or otherwise) the I Phone [sic] 7 plus with serial number ********** and cellular phone number ******* pursuant to Indiana Code 35-33-5-11(a) and that if she fails to comply with this order, that she be subject to the contempt powers of the court.

You are further authorized to deliver any of said items to an appropriate facility for analysis and comparison against other evidence gathered in the investigation.

Appellant's App. p. 49.[3]

[8] On August 15, 2017, Seo, now represented by counsel, notified the State that she would not comply with the order to unlock the phone. Accordingly, the State filed a motion that same day for a rule to show cause why Seo should not be held in contempt. The trial court held a hearing on the matter on September 21, 2017. At the conclusion of the hearing, the trial court entered an order finding Seo in contempt, which reads in relevant part as follows:

> 1. The State requested and the Court granted a search warrant for the contents of the phone at issue (iPhone 7 plus bearing serial number **********, previously connected with number **********) under cause number 29D01-1708-MC-

[3] The probable cause affidavit supporting the issuance of this search warrant is not in the record before us.

5624, and the Court took Notice of such cause for the purpose of ruling in this cause.

2. The State requested and the Court granted a search warrant compelling the Defendant to unlock the phone by biometric fingerprint access, keycode, password, passcode, or otherwise under cause number 29D01-1708-MC-5640.

3. The Court finds that the statutory requirements as found in Ind. Code 35-33-5-11 have been satisfied in this cause.

4. The act of unlocking the phone does not rise to the level of testimonial self-incrimination that is protected by the Fifth Amendment of the United States Constitution or by Article 1, Section 14 of the Indiana Constitution.

5. Katelin Eunjoo Seo is found to be in contempt of Court for failure to abide by the warrant issued under this cause: 29D0l-1708-MC-5640.

IT IS THEREFORE ORDERED, ADJUDGED AND DECREED as follows:

1. That Katelin Eunjoo Seo is **ORDERED** incarcerated in the Hamilton County Jail and she shall surrender herself at the Hamilton County Jail no later than 4:30 p.m. on today's date, Friday, September 22 unless and until she purges herself of Contempt of Court.

2. That in order to purge herself of Contempt of Court, Katelin Eunjoo Seo is **ORDERED** to unlock the phone at issue *and* to (1) disable the passcode function on the phone, *or* (2) to change the passcode on the phone to 1234.

Appellant's App. pp. 6–7 (emphases in original).

[9] The same day that the trial court entered its contempt order, Seo filed a motion to stay the contempt sanction pending appeal, which the trial court granted on September 25, 2017. Seo filed a notice of appeal on October 20, 2017.[4]

I. Standard of Review

[10] The determination of whether a party is in contempt of court is a matter within the sound discretion of the trial court. *Jones v. State*, 847 N.E.2d 190, 199 (Ind. Ct. App. 2006), *trans. denied*. However, here, the question is whether forcing Seo to unlock her phone or reveal her password is a violation of her Fifth Amendment right against self-incrimination, and this is a pure question of law that is reviewed *de novo*. *See United States v. Neighbors*, 590 F.3d 485, 492 (7th Cir. 2009) (holding that the question of whether voice identification based on in-court proceedings for a criminal defendant violated his Fifth Amendment right against self-incrimination was a question of law reviewed *de novo*); *Conn v. State*, 89 N.E.3d 1093, 1097 (Ind. Ct. App. 2017) (noting that pure questions of law are reviewed *de novo*), *trans. denied*.

II. Encryption

[11] Because this case involves the technical aspects of locking and unlocking a modern smartphone, and the current caselaw considers the method of unlocking that information somewhat dispositive as to whether unlocking can

[4] We held oral argument on this case on May 1, 2018. We commend counsel for the quality of their written and oral advocacy.

be coerced, a brief overview of the underlying technology is in order. One law review note succinctly summarizes encryption as follows:

> Encryption is the process of concealing information, and all such systems have several similar characteristics. At its most basic level, encryption involves transforming information or data, called "plaintext," into a coded form that cannot be understood by outsiders. The process is performed according to the encryption algorithm, a set of rules that governs how the plaintext is transformed. While this can be as simple as substituting each letter in a message with a corresponding number, modern encryption algorithms often consist of a complex series of mathematical functions. Regardless of the manner of encryption, the result is that the plaintext is made unintelligible to outsiders.

Andrew J. Ungberg, *Protecting Privacy Through a Responsible Decryption Policy,* 22 Harv. J.L. & Tech. 537, 540 (2009) (citation footnotes omitted).[5] Another commentator further explains:

> When . . . [data] is encrypted using current technology an "encryption key" is required to decrypt the message. An encryption key is basically a very long string of numbers that is stored in the encryption software's memory. The software users do not have to remember this long number; instead [they] can enter a more easily remembered password or passphrase, which in turn activates the encryption key. When the government seeks to compel an ordinary citizen to turn over the means by which he

[5] For a more detailed look at encryption and possible ways to defeat encryption, see Orin S. Kerr and Bruce Schneier, *Encryption Workarounds* (March 22, 2017), 106 Geo. L.J. 989 (2018).

> can decrypt the data, the disclosure order will typically compel him to turn over his password rather than the encryption key.

Michael Wachtel, *Give Me Your Password Because Congress Can Say So*, 14 U. Pitt. J. Tech. L. & Pol'y 44, 48 (2013) (citations and quotations omitted).

III. iPhone Security[6]

[12] The iPhone 7 Plus at issue here is locked, and therefore, the contents of the phone are encrypted. *See* Apple, *iOS Security* p. 14 (Jan. 2018).[7] That is, even if the digital contents of the phone's storage could be extracted from the phone, those contents would still be undecipherable without also unencrypting the contents.

[13] The contents of the iPhone 7 series are encrypted with a strong 256-bit AES encryption key.[8] Instead of requiring each user to memorize a 256-bit key, the key is instead itself encrypted with a "system key" unique to each phone, plus

---

[6] The discussion that follows is focused on the smartphone at issue in this case, an iPhone 7 Plus. However, the substance of the discussion also applies to smartphones manufactured under other brand names, generally, and, in some instances, specifically.

[7] https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[8] AES stands for "Advanced Encryption System." *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 927 (N.D. Cal. 2009). A 256-bit AES encryption key is almost unfathomably strong because there are 2^{256} possible keys. 2^{256} is approximately equivalent to 10^{77}. By way of comparison, scientists estimate that there are 10^{86} (one-hundred thousand quadrillion vigintillion) *atoms* in the entire *universe*. *See* John Carl Villanueva, *How Many Atoms Are There in the Universe?* (Apr. 22, 2018), https://www.universetoday.com/36302/atoms-in-the-universe/. Thus, guessing a 256-bit key is effectively impossible. *See* Kerr & Schneier, *supra* at 994 (noting that cracking a 256-bit key is "beyond the reach of any foreseeable computer technology," thus rendering a "brute force" repeated guessing of the key "effectively impossible."). But the implementation of an encryption system may contain errors that allow someone to bypass this seemingly unbreakable security. *Id.* at 1005–06.

the user-chosen passcode. *Id*. When a user enters her passcode, this is combined with the system key to unlock the "File System Key," which is used to decipher the contents of the phone.[9] *Id.*

[14] Thus, each time a user unlocks her phone, she is enabling the phone to recreate *all* of the information on the phone, taking what was once indistinguishable from random noise and deciphering it into the requested data. *See* Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. Pub. Int. L.J. 53, 59 (2015) (discussing the process of on-the-fly encryption and decryption).

---

[9] More precisely, a file written to the storage on the iPhone can be of one of four different "Data Protection Classes," as assigned by the app that creates it. *Apple, iOS Security* p. 15. Files that are in the "Complete Protection" class are protected by a class key derived from the user passcode and the phone's unique identifier ("UID"). "Shortly after the user locks a device . . . the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks the device using Touch ID or Face ID." *Id*. Files created in the "Protected Unless Open" class are those that need to be written even when the device is locked, such as an email attachment downloading in the background. *Id*. at 16. Such files are encrypted using a per-file asymmetric key, and the public key is stored with the encrypted per-file key. *Id*. When a file in this class is closed, the per-file key is wiped from memory. *Id*. "To open the file again, the shared secret is re-created using the Protected Unless Open class's private key and the file's ephemeral public key, which are used to unwrap the per-file key that is then used to decrypt the file." *Id*.

The third class is the "Protected Until First User Authentication." *Id*. "This class behaves in the same way as Complete Protection, except that the decrypted class key isn't removed from memory when the device is locked." *Id*. Instead, the key is removed only on reboot. *Id*. "The protection in this class has similar properties to desktop full-volume encryption, and protects data from attacks that involve a reboot." *Id*. This is the default class for all third-party app data not otherwise assigned to a Data Protection class.

The final class is "No Protection," and is protected only with the UID. *Id*. "Since all the keys needed to decrypt files in this class are stored on the device, the encryption only affords the benefit of fast remote wipe." *Id*. However, "[i]f a file isn't assigned a Data Protection class, it is still stored in encrypted form (as is all data on an iOS device)."

In the present case, there is nothing in the record to indicate which app created the information sought by the State, nor under which Data Protection class the data sought falls within.

[15] Randomly guessing the passcode (a "brute force" attack) can be automated and accomplished at mind-boggling speeds by modern computers. *See* Paul Roberts, *Update: New 25 GPU Monster Devours Passwords in Seconds*, Security Ledger (Dec. 4, 2012, 19:12) (reporting on a password-guessing cluster of computer graphics cards that can guess 348 billion password hashes per second).[10] But such brute force attacks are difficult because of the iPhone's software security features, which incrementally increases the time allowed between such guesses. Apple, *iOS Security* p. 15. This eventually allows only one guess every hour, or, depending upon the settings of the phone, wipes the contents of the phone after ten incorrect guesses, making repeated guessing of the password impractical.

[16] Thus, if the police want or need to gain access to an iPhone, the cooperation of its owner is practically a necessity. But if the owner of the smartphone is unwilling to cooperate with the police, then the police are faced with fewer options. One of these options has been to attempt to bypass the encryption via some error in the implementation of the encryption. The other has been to use the power of the courts to compel the owner to unlock the phone. This case presents the question of when the owner of the phone may refuse to cooperate with the police based upon her rights not to incriminate herself found in the U.S. Constitution.

---

[10] https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/

IV. The Fifth Amendment and Testimony

[17] Seo claims that the trial court's order compelling her to unlock her phone[11] violates her right under the Fifth Amendment[12] not to be a witness against herself. This appears to be a case of first impression in Indiana.

[18] The Self-incrimination Clause of the Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself[.]" U.S. Const. amend. V. This constitutional safeguard is applicable to state criminal cases by way of the Fourteenth Amendment. *Bleeke v. Lemmon*, 6 N.E.3d 907, 925 (Ind. 2014) (citing *Withrow v. Williams*, 507 U.S. 680, 688–89 (1993)). The Fifth Amendment prohibits compelled testimony that is incriminating. *Id*. (citing *Hiibel v. Sixth Judicial Dist. Ct. of Nev.*, 542 U.S. 177, 190 (2004)). Thus, the government cannot force someone to provide a communication that is "testimonial" in character. *In re Search Warrant*

---

[11] We take judicial notice that Seo's iPhone 7 Plus is equipped with what Apple refers to as "Touch ID," a biometric fingerprint sensor that can be used to unlock the phone, instead of a typed-in password. *See* iPhone 7 Technical Specifications, https://www.apple.com/iphone-7/specs/ (last visited August 13, 2018); Apple, *iOS Security* p. 7. The record is unclear as to which method of security Seo chose to use. *See* Tr. p. 9 (describing the phone as "locked," but not indicating which method could be used to unlock it). However, the search warrant applied to either method. *See* Appellant's App. p. 49 (order compelling Seo to unlock her phone "via biometric fingerprint, passcode, password, or otherwise[.]").

[12] Seo has yet to make any Fourth Amendment claim regarding the validity of the search warrant. Given the early procedural posture of this case, we express no opinion as to the validity of the search warrant issued by the trial court, as that issue has yet to be litigated in the first instance. We also note that Seo does not make any separate argument under the anti-self-incrimination provision of the Indiana Constitution, other than to mention the Indiana Constitution in her conclusion. We therefore focus our analysis solely on the Fifth Amendment of the Constitution of the United States. *See Holloway v. State*, 69 N.E.3d 924, 931 (Ind. Ct. App. 2017) (noting that a defendant cannot invoke analysis of an issue under the Indiana Constitution without a separate and independent analysis of the claim), *trans. denied*.

Application for [redacted text], 279 F.Supp.3d 800, 803 (N.D. Ill. 2017) (citing *United States v. Hubbell*, 530 U.S. 27, 34 (2000)).

[19] The Fifth Amendment privilege against self-incrimination reflects our nation's "fierce 'unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt,' that defined the operation of . . . [Great Britain's] Star Chamber, wherein suspects were forced to choose between revealing incriminating private thoughts or forsaking their oath by committing perjury." *Pennsylvania v. Muniz*, 496 U.S. 582, 596 (1990) (quoting *Doe v. United States*, 487 U.S. 201, 212 (1988) ("*Doe II*")). Indeed, "[t]he Fifth Amendment privilege against compulsory self-incrimination . . . protects 'a private inner sanctum of individual feeling and thought and proscribes state intrusion to extract self-condemnation.'" *Id*. (quoting *United States v. Nobles*, 422 U.S. 225, 233 (1975)).

[20] To date, the United States Supreme Court has issued no opinion directly addressing whether compelling a person to unlock a phone or provide a passcode is testimonial.[13] However, in a series of cases, the Court has explored whether certain acts of producing documents can be testimonial for Fifth Amendment purposes. Importantly, these cases span more than a century and

[13] The Court has held that there is no Fifth Amendment problem with compelling a person to do something that displays a *physical* characteristic that might be incriminating. *See Hubbell*, 530 U.S. at 35. Among the compelled physical characteristics that have been held to be non-testimonial are fingerprints. *Schmerber v. California*, 384 U.S. 757, 763–65 (1966)); *United States v. Hook,* 471 F.3d 766, 773–74 (7th Cir. 2006). This reasoning is outdated and ironic when compared with the current, heightened, "state of the art" electronic security provided by physical characteristics such as facial recognition and retinal scans.

contain important developments during times when the internet and smartphones did not exist.

[21] In the late 1800s, the Court held in *Boyd v. United States*, 116 U.S. 616, 633 (1886), that "[w]e have been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself."[14] In *Fisher v. United States*, 425 U.S. 391 (1976), however, the Court backed away from its earlier holding in *Boyd*, but never expressly overruled its prior holding. *See Fisher*, 425 U.S. at 407 (stating that "[s]everal of *Boyd*'s express or implicit declarations have not stood the test of time."). Still, in *Schmerber v. California*, 384 U.S. 757, 763–64 (1966), the Court cited *Boyd* when holding that "[i]t is clear that the protection of the [Fifth Amendment] privilege reaches an accused's communications, *whatever form they might take*, and the compulsion of responses which are also communications, for example, compliance with a subpoena to produce one's papers." (emphasis added).

[22] The *Fisher* Court proceeded to examine the question of what kinds of acts of production are "testimonial." *Fisher* involved two consolidated cases in which the IRS served summonses on two attorneys, directing the attorneys to produce documents obtained by their clients relating to tax returns. Both attorneys argued *inter alia* that this would violate their clients' rights against self-

---

[14] *See also Carpenter v. United States*, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting) (citing Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of Boyd*, 74 N.Y.U.L. Rev. 1575, 1605–23 (1999); *Rex v. Purnell*, 96 Eng. Rep. 20 (K.B. 1748); Christopher Slobogin, *Privacy at Risk* 145 (2007)).

incrimination. The Court held that the Fifth Amendment privilege could apply to situations where a defendant is compelled to produce incriminating evidence, and that the act of producing even unprivileged evidence can have communicative aspects itself and may be testimonial, entitling it to Fifth Amendment protection. *Id*. at 409–10. Nevertheless, the Court noted that the Government was "in no way relying on the 'truth-telling' of the taxpayer to prove the existence of or his access to the documents," and the production of the documents did not authenticate the documents, because they had been produced by accountants and not the taxpayers being investigated themselves. *Id*. at 411.

[23] The Court further held that, because the existence, location, and authenticity of the evidence sought was known to the government, the Fifth Amendment privilege was inapplicable because the contents of the individual's mind was not used against him. *See id*. ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").[15] Thus, the Fifth Amendment privilege did not apply to the third-party production of documents requested in *Fisher*. *Id*. at 414.

---

[15] This is known as the "foregone conclusion" doctrine. Andrew T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*, 39 Rutgers Computer & Tech. L.J. 194, 197 (2013). Many cases involving encryption have been decided under the foregone conclusion doctrine, a doctrine outstripped by technology, as discussed in more detail below.

[24] The Court in *Doe II* considered the legality of an order compelling the target of a grand jury investigation to authorize foreign banks to disclose records of his accounts. 487 U.S. at 202. The target of the investigation argued that compelling him to sign the consent form would give the government access to potentially incriminating records that would otherwise be unavailable to it, due to the fact that the District Court had no power to order foreign banks to produce the documents. *Id*. at 204. The Court rejected this argument and held that "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Id*. at 210.

[25] Justice John Paul Stevens dissented, and in its acknowledgement of his dissent, the majority famously noted:

> We do not disagree with the dissent that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. *In our view, such compulsion is 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 (quoting *id*. at 219 n.1 (Stevens. J., dissenting) (emphasis added).

[26] Twelve years later, but before the advent of smartphones and a robust internet, the Supreme Court again revisited this issue in *United States v. Hubbell*, 530 U.S. 27 (2000), a case that arose out of the Whitewater investigation. The target in that case, Webster Hubbell, had pleaded guilty to charges of mail fraud and tax

evasion arising out of his billing practices. *Id*. at 30. In the plea agreement, Hubbell promised to provide the Independent Counsel with "full, complete, accurate, and truthful information" about matters relating to the Whitewater investigation. *Id*.

[27] Later, while Hubbell was serving his twenty-one-month prison sentence, a grand jury issued a *subpoena duces tecum* demanding the production of eleven categories of documents. *Id*. at 31. Hubbell invoked his Fifth Amendment privilege. *Id*. The Independent Counsel then produced an order from the District Court directing Hubbell to comply with the subpoena and granting him immunity against the government's use and derivative use of the compelled testimony. *Id*. Hubbell then delivered the specified documents and yet was subsequently indicted again for various wire fraud, mail fraud, and tax crimes. *Id*. The District Court dismissed this new indictment based on the violation of the immunity previously granted. *Id*. at 32. The United States Court of Appeals for the District of Columbia Circuit reversed and remanded, and the Supreme Court granted *certiorari*.

[28] The Supreme Court, citing *Fisher*, reiterated that "a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege." *Id*. at 35–36. Accordingly, the simple fact that the documents contained incriminating evidence did not mean that Hubbell could avoid complying with the subpoena. *Id*. at 36.

[29] Importantly, however, the Court made it clear that the very act of producing documents in response to a subpoena may have a compelled testimonial aspect in and of itself. *Id*. "The 'compelled testimony' that is relevant . . . is not to be found in the *contents* of the documents produced in response to the subpoena. *It is, rather, the testimony inherent in the act of producing those documents*." *Id*. at 40 (emphasis added).

[30] In discussing the government's subpoena, which had required the defendant to provide numerous responses to very broad requests, the Court stated that "[t]he 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 43. The Court then held that the "foregone conclusion" rationale did not apply to overcome the testimonial aspects of Hubbell's production of documents because the government could not identify the files, describe what they were, tell whether they existed, or whether Hubbell had knowledge of, possession of, or access to them. *See id*. at 45 ("here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent."). Only Hubbell's responses had provided the government with this information. *See id*. at 43 ("It was 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."). The Court concluded that the Fifth Amendment privilege did apply and that the grant of immunity extended to the

use and derivative use of the testimonial aspects of the production of those documents. *Id*.

[31] We acknowledge that the United States Supreme Court has backtracked from its earlier pronouncements that the protections afforded by the Fifth Amendment, in addition to the Fourth Amendment, implicated privacy concerns. Indeed, the *Fisher* Court noted that although it had "often stated that one of the several purposes served by the constitutional privilege against compelled testimonial self-incrimination is that of protecting personal privacy," it then held that "[w]e cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy—a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against compelled self-incrimination, not [the disclosure] of private information." 425 U.S. at 399–401; *see also United States v. Doe*, 465 U.S. 605, 618 (1984) ("*Doe I*") (O'Connor, J., concurring) ("The notion that the Fifth Amendment protects the privacy of papers originated in *Boyd* [], but our decision in *Fisher* [], sounded the death-knell for *Boyd*.").

[32] Still, courts continue to acknowledge that the Fifth Amendment's anti-self-incrimination provision "protect[s] privacy in the sense of confidentiality." *See Willan v. Columbia Cty.*, 280 F.3d 1160, 1163 (7th Cir. 2002). Thus, while we do not consider the Fifth Amendment as a "general protector of privacy," we cannot ignore the privacy/confidentiality implications that compelled revelation of a smartphone passcode would inevitably have based on the

extraordinary quantitative and qualitative differences between the amount of digital information stored on a smartphone compared to traditional paper-based media. *See* Section VI, *infra.* We believe that legal analysis of digital information storage must change, and soon, in order to be relevant and credible. *See* Section VI and Section VIII, *infra.*

V. The Testimonial Nature of a Passcode

[33] Under current, paper-based legal analysis, Seo argues that her passcode is testimonial in nature, and that compelling her to reveal it, or compelling her to unlock the phone using the passcode, would be a testimonial act that she cannot be compelled to do without violating her Fifth Amendment privilege. Contrasting the facts of the present case with those in *Doe II*, Seo notes that she is being compelled to do more than merely sign a consent form to obtain records from a third party; she is instead being compelled to reveal the *contents of her own mind*—her password. She also argues that compelling her to reveal her password is more invasive than just requiring her to assemble documents, which was found to be testimonial in *Hubbell*. She is instead being compelled to give the State access to the entire contents of her mobile phone, which in all probability contains a wealth of digital information completely unrelated to the focus of law enforcement needs in her case.

[34] The State contends that the Fifth Amendment is not implicated by the trial court's order because it does not compel Seo to reveal the password to the State; it simply requires her to unlock the phone using her password (or other method) and disable the password feature so that the State may continue to access it.

Accordingly, the State argues, Seo need not reveal the password, and therefore the "contents of her mind," to the State at all. Therefore, according to the State's argument, the foregone conclusion doctrine from *Fisher* controls.

[35] Many courts that have considered this issue have held that forcing a person to reveal their password is testimonial because, in the words of the *Doe II* Court, it is "[t]he expression of the contents of an individual's mind." 487 U.S. at 210 n.9; *see also United States v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010) (holding that the government could not compel the defendant to reveal his password because this amounted to "testimony" from him which would "requir[e] him to divulge through his mental processes his password."); Kiok, *supra* at 76 ("Because a password comes from a defendant's mind, its revelation is testimonial.").

[36] Indeed, when addressing Justice Stevens's dissent in *Doe*, the majority of the Court noted that compelling the defendant in that case to sign the bank disclosure forms was more akin to "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it was to "be[ing] compelled to reveal the combination to [petitioner's] wall safe." 487 N.E.2d at 210 n.9. Here, under precedent as it now exists, we hold that the State is seeking the electronic equivalent to a combination to a wall safe—the passcode to unlock the iPhone.

[37] Moreover, some courts appear to have rejected the State's attempt to distinguish between compelling a defendant to reveal the passcode versus

merely compelling the defendant to unlock the phone herself and give the State access to the unlocked phone. As summarized by one commentator:

> But what about forcing you to enter a password? Is this a compellable physical act? Three courts have answered no. In their view, forcing a person to use a password to decrypt a hard drive is not a physical act because it forces the person to use the contents of his mind. Also prevalent in these courts' reasoning is the key-combination dicta already discussed: "A password, like a combination, is in the suspect's mind, and is therefore testimonial . . . ."

Dan Terzian, *The Micro-Hornbook on The Fifth Amendment and Encryption*, 104 Geo. L. J. Online 168, 171–72 (2016).

[38] The three cases Terzian refers to are: *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012), which held that "the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature."; *In re Boucher*, 2007 WL 4246473, at *3 (D. Vt. Nov. 29, 2007),[16] which held that entering a password into a computer implicitly communicates facts and was therefore testimonial in nature; and *Commonwealth v. Baust*, 89 Va. Cir. 267 (2014), which held that compelling defendant to provide access to his locked phone through his

[16] The initial decision in *Boucher* was issued by the District Court Magistrate, whose decision was overturned by the District Court Judge in the subsequent decision. But the subsequent decision was based on the "foregone conclusion" doctrine. *See In re Boucher*, 2009 WL 424718 at *3 (D. Vt. Feb. 19, 2009) (citing *Fisher*, 425 U.S. at 411).

passcode was testimonial. *See also* Kiok, *supra* at 76 ("an order to compel decryption [i.e., unlocking a smartphone] compels a testimonial act."); Andrew T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in The Technological Era*, 39 Rutgers Computer & Tech. L.J. 194, 209 (2013) ("Entering a password or otherwise decrypting the contents on a computer is a testimonial act that receives the full protection of the Fifth Amendment.").[17]

[39] Upon consideration of this authority, and because we believe that electronic data and the devices that contain it are fundamentally different than paper documents and paper storage, we reject the State's attempt to distinguish between compelling Seo to convey her passcode to the State and compelling Seo to simply unlock her phone by entering the passcode itself. It is a distinction

[17] Interestingly, some courts have made a distinction between compelling a person to unlock a phone using a password and compelling a person to unlock a phone using a fingerprint. As noted above, the Supreme Court has held that forcing someone to submit to the taking of fingerprints is not testimonial. *Schmerber*, 384 U.S. at 764; *see also Hook*, 471 F.3d at 773–74. Because of this, at least two courts have held that there is no Fifth Amendment problem with compelling a defendant to produce a fingerprint to unlock a smartphone. *Baust*, 89 Va. Cir. 267, at *4; *State v. Diamond*, 905 N.W.2d 870, 878 (Minn. 2018). As noted*, supra*, it is the height of irony that the most secure current forms of electronic identification, the fingerprint, and more recently, facial recognition or retinal scans, currently have no protection against compulsory use by law enforcement authorities under *Schmerber et al*. This difference is reflective of legal thinking from a paper-based world that courts currently are called upon to stretch to fit a world of electronic data about everything and everyone. Our courts need a new paradigm that reflects our modern world.

However, even the fingerprint-unlocking function of the iPhone 7 at issue here will become inoperative after forty-eight hours, thereby requiring the use of a passcode. *See* Terzian, 104 Geo. L. J. Online at 169 (citing Apple*, About Touch ID Advanced Security Technology* (Sept. 11, 2017) (noting that a fingerprint alone is insufficient to unlock an iPhone when "more than 48 hours have elapsed from the last time" the phone was unlocked). Here, it has been well more than forty-eight hours since Seo's phone has been unlocked by the fingerprint sensor. Thus, even though the State might be able to compel Seo to attempt to use her fingerprint to unlock the phone, this would, in all likelihood, be unsuccessful.

without a difference because the end result is the same: the State is compelling Seo to divulge the contents of her mind to obtain incriminating evidence.

[40] Furthermore, we consider Seo's act of unlocking, and therefore decrypting the contents of her phone, to be testimonial not simply because the passcode is akin to the combination to a wall safe as discussed in *Doe*. We also consider it testimonial because her act of unlocking, and thereby decrypting, her phone effectively recreates the files sought by the State. As discussed above, when the contents of a phone, or any other storage device, are encrypted, the cyphertext is unintelligible, indistinguishable from random noise. In a very real sense, the files do not exist on the phone in any meaningful way until the passcode is entered and the files sought are decrypted. Thus, compelling Seo to unlock her phone goes far beyond the mere production of paper documents at issue in *Fisher*, *Doe*, or *Hubbell*. Because compelling Seo to unlock her phone compels her to literally recreate the information the State is seeking, we consider this re-creation of digital information to be more testimonial in nature than the mere production of paper documents.

[41] Stripping legal precedent away from the issue, the very nature of a passcode supports the conclusion that it is the product of one's mind. Many people choose a passcode that is uniquely memorable to them in some way. Often, the password is an important date or other bit of information they hope will not be easily guessed, but that is still uniquely memorable to them. To force Seo to reveal her passcode is the very definition of compelling her to reveal the

contents of her mind. Accordingly, we hold that compelling Seo to unlock her phone in any manner is testimonial.[18]

VI. The "Foregone Conclusion" Doctrine

[42] The State and the dissent argue that compelling Seo to unlock her phone is not a violation of the Fifth Amendment privilege because of the "foregone conclusion" doctrine. "Even if a response is testimonial, the privilege does not apply where the testimonial portion is a foregone conclusion." Dan Terzian, *Forced Decryption as a Foregone Conclusion,* 6 Cal. L. Rev. Cir. 27, 28 (May 2015). Under the "foregone conclusion" doctrine:

> the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a "foregone conclusion" that "adds little or nothing to the sum total of the Government's information." [*Fisher*, 425 U.S. at 411]. For the rule to apply, the Government must be able to "describe with reasonable particularity" the documents or evidence it seeks to compel. [*Hubbell*, 530 U.S. at 30].

United States v. Apple MacPro Computer, 851 F.3d 238, 247 (3d Cir. 2017); *see also* Kerr & Schneier, *supra* at 1002 ("The foregone conclusion doctrine teaches that,

---

[18] For the Fifth Amendment privilege to apply, the testimony at issue must also be incriminating. *Bleeke*, 6 N.E.3d at 925 (citing *Hiibel*, 542 U.S. at 190). Here, neither party disputes that the information the State seeks from Seo's iPhone would be incriminating. Moreover, given the vast amounts of personal information located on a typical smartphone, there should be a reasonable presumption that *something* incriminating would be discovered during review of the contents of almost anyone's smartphone. Consider the expansive law enforcement claims that could be made under the plain view doctrine or the good faith exception to the Fourth Amendment or Article 1 Section 11 of the Constitution of Indiana protections when searching a smartphone. *See* note 26, *infra*.

if the testimonial aspect of production is already known to the government and is not to be proven by the testimonial act, then the testimony is a foregone conclusion and the Fifth Amendment privilege does not apply.").[19]

[43] "Although the State need not have 'perfect knowledge' of the requested evidence," for the foregone conclusion rationale to apply, "it 'must know, and not merely infer,' that the evidence exists, is under the control of defendant, and is authentic." *State v. Stahl*, 206 So.3d 124, 135–36 (Fla. Dist. Ct. App. 2016) (citing *United States v. Greenfield*, 831 F.3d 106, 116 (2d Cir. 2016)) (emphasis removed). Thus, where the foregone conclusion rationale applies, the question is not of testimony, but of surrender. *Id*. at 136 (citing *Fisher*, 425 U.S. at 411).

[44] In this sense, the foregone conclusion doctrine of Fifth Amendment jurisprudence contains its own requirement of specificity regarding the information sought from the defendant, i.e., that the State or government be able to describe with reasonable particularity the documents or evidence it seeks to compel. Very importantly, this particularity requirement prevents the foregone conclusion exception from swallowing the rule by requiring that the State already know the documents or evidence it seeks. So long as the State already knows with reasonable particularity the documents or evidence it seeks, the surrender of the evidence "adds little or nothing to the sum total of the

---

[19] There appears to be some confusion as to whether the foregone conclusion rationale is a true exception to the Fifth Amendment privilege as it applies to testimonial production of documents, or whether the foregone conclusion rationale means that the production of the documents at issue is simply not testimonial. Either way, however, if the foregone conclusion doctrine is applicable, under current precedent, there is no Fifth Amendment protection.

Government's information." *Fisher*, 425 U.S. at 411. In contrast, where the State does not already know the evidence exists, it cannot describe with reasonable particularity the evidence it seeks, and the foregone conclusion exception will not apply.

[45] The State argues that the foregone conclusion should apply under the facts of the present case. The State focuses its argument not on the *contents* of the phone, but on the passcode itself. Specifically, the State claims, "the act of unlocking a cell phone contains only one implied fact: the person knows the password to the phone, which by inference says that the person has control over and possession of the phone." Appellee's Br. at 19. The State therefore contends that the foregone conclusion rationale should apply because "a person must know her passcode to use her own phone, *the testimony implicit in the act of unlocking the phone* is a foregone conclusion when the State has proven that the phone belongs to her." *Id*. at 22 (emphasis added).

[46] There is some support for the State's position. Indeed, it is one of the two paths of legal analysis using a paper-based analogy. For example, in *State v. Stahl*, the court held that, in deciding whether providing a passcode to a locked phone fell within the ambit of the foregone conclusion doctrine, "the relevant question is whether the State has established that it knows with reasonable particularity *that the passcode exists*, is within the accused's possession or control, and is authentic." 206 So.3d at 136 (emphasis added); *see United States v. Spencer*, ___ F.Supp.3d ___, 2018 WL 1964588 at *3 (N.D. Cal. April 26, 2018) (holding that, to determine whether the foregone conclusion doctrine applied, the

appropriate question was whether the government could show that it was a foregone conclusion that the defendant could decrypt the devices); *Commonwealth v. Davis*, 176 A.3d 869, 876 (Pa. Super. Ct. 2017) (holding that the foregone conclusion doctrine applied where the state was able to show that it knew that the *passcode* existed, it was within the defendant's possession or control, and was authentic); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (concluding that the "factual statements that would be conveyed by the defendant's act of entering an encryption key in[to] the computers [were] 'foregone conclusions[.]'"); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1236–37 (D. Colo. 2012) (holding that the foregone conclusion doctrine applied where the State had evidence proving the encrypted computer belonged to the defendant and that she knew the password).

[47] However, Seo argues the other path of the paper-based legal analogy: the foregone conclusion doctrine does *not* apply here because the State cannot describe with reasonable particularity the digital files or evidence it seeks to compel her to produce. That is, Seo argues that the focus of the foregone conclusion analysis is not whether it is a foregone conclusion that Seo knows her own passcode; rather, the focus should be on whether the State can describe with reasonable particularity the digital information it seeks to compel her to produce. *See Apple MacPro Computer*, 851 F.3d at 247 (citing *Hubbell*, 530 U.S. at 30). And there is support for Seo's framing and application of the foregone conclusion doctrine in other jurisdictions that have considered her argument.

[48] In *Commonwealth v. Baust,* the court held that *the password* itself was not a foregone conclusion because it was not known outside of the defendant's mind. 89 Va. Cir. 267 at *4. Presaging Seo's argument here, the *Baust* court held that, "[u]nlike a document or tangible thing, such as an unencrypted copy of the footage itself, if the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it." *Id.*; *see also In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1347 (holding that the foregone conclusion doctrine was inapplicable where the government had not shown that it possessed knowledge as to the "files on the [encrypted] hard drives at the time it attempted to compel production."); *Sec. & Exch. Comm'n v. Huang*, 2015 WL 5611644, at *4 (E.D. Pa. Sept. 23, 2015) (holding that the foregone conclusion doctrine did not apply because the SEC had no evidence any digital files it sought were actually located on the target's work-issued smartphones).

[49] With an eye toward a more comprehensive rethinking of the legal analysis regarding digital information and storage, we believe these cases express the better rationale.[20] What is being compelled here is not merely the passcode. As described above, compelling Seo to enter her password forces her to effectively re-create the entire contents of her phone. In the words of the Third Circuit

[20] This is one of the two available rationales under the outdated paper paradigm that our courts are stumbling through in an effort to resolve information production disputes regarding electronic data on electronic devices. Judge May in her dissent chooses the opposite alternative. We believe the alternative branch of cases we have chosen contains the better rationale because it not only resolves the instant issue and case; it also presages a suggested way forward in this important and continually evolving area.

Court of Appeals, the State must be able to describe with reasonable particularity the digital files it seeks to compel. *Apple MacPro Computer*, 851 F.3d at 247 (citing *Hubbell*, 530 U.S. at 30). Here, what the State seeks to compel is not merely the password, but the entire contents of Seo's iPhone. Thus, for the foregone conclusion doctrine to apply, the State must be able to describe with reasonable particularity the *discrete* contents on Seo's phone—e.g., all texts to D.S. created on Seo's iPhone—that it is compelling her to not only produce, but to re-create by entering her passcode and decrypting the contents of the phone. This is a burden the State has not met.

[50] To be sure, the investigating detective has already viewed Seo's phone and has seen information that caused him to believe that D.S. was the victim of stalking and harassment by Seo. Indeed, Detective Inglis testified that he made a "forensic download" of the contents of Seo's phone. Tr. p. 6. We may therefore presume that the State already has *much* of the information contained on Seo's phone.[21] But it is not this information the State now seeks to compel. Instead, what the State seeks now is evidence that might have been created on Seo's

[21] We also note that the information the State seeks is not of an emergency nature, or of a completely new description or character from that information it already has. The State could potentially prove its case entirely from the text messages received by D.S. and that may still be found on his cellphone, comparing the alleged threats and harassment language after the protective order was issued to the threatening and harassing texts contained in its forensic download of Seo's cellphone with her consent. The State has also not shown that it has tried unsuccessfully to obtain the desired information through readily available and far less constitutionally intrusive methods, such as third-party subpoenas to Seo's cell carrier regarding the texts at issue or to Apple to inquire as to what applications she has downloaded, with an eye toward those apps or services that could mask her cellphone number. A subpoena to Google could also reveal any Google Voice numbers Seo has secured, and the State could compare those numbers to the sources of the texts to D.S.

phone *after* this forensic download, i.e., evidence that Seo sent the flood of threatening and harassing messages to D.S. But again, the State has not described with *any* particularity the digital information it seeks to access.

[51] We acknowledge that the State secured a search warrant for the contents of Seo's iPhone. However, this warrant did not describe with any reasonable particularity the digital information the State sought to find, as the Fifth Amendment requires.[22] Instead, the warrant merely stated that the police were:

> authorized and ordered in the name of the State of Indiana, with necessary and proper assistance, in the daytime or nighttime, to search the property located at and described as:
>
> 5. for purpose of searching items described in the sworn evidence, to wit:
>
> > That Katelin Eunjoo Seo be compelled to unlock (via biometric fingerprint, passcode, password, or otherwise) the I Phone [sic] 7 plus with serial number ********** and cellular phone number ******* pursuant to Indiana Code 35-33-5-11(a) and that if she fails to comply with this order, that she shall be subject to the contempt powers of the court.

---

[22] We decline to address whether the issuance of a search warrant is sufficient to meet the State's burden under the foregone conclusion doctrine to describe with reasonable particularity the digital files or evidence it seeks to compel. The Fourth Amendment requirement for probable cause requires only that the magistrate issuing the warrant make a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *State v. Spillers*, 847 N.E.2d 949, 952–53 (Ind. 2006). This appears to us to be a lower standard than that required for the foregone conclusion doctrine to apply, i.e., that the government be able to describe with "reasonable particularity" the documents or evidence it seeks to compel. *Hubbell*, 530 U.S. at 44–45. Moreover, here, there has yet to be a challenge to the propriety of the warrant. Indeed, such a challenge would likely come only after the State has searched the phone, discovered incriminating evidence, if any, and attempts to use that evidence at trial.

Appellant's App. p. 49.

[52] Thus, the warrant itself does not describe with any particularity the digital information the State seeks to compel Seo to produce or the evidence the State is authorized to search for.[23] Nor does the trial court's order on contempt describe with any reasonable particularity the digital information the State seeks to compel.[24]

[53] Going forward the State can, and should, describe the information it seeks and the programs that contain it on Seo's cellphone, e.g., any texts between Seo and D.S., whether in Apple's Message application, Facebook, Twitter or otherwise, and the contents of any application that allows a user to change the apparent telephone number originating an electronic communication, such as Google Voice or Pinger. And perhaps more importantly, in its order the court should also require the State to limit its search within messaging to variations of D.S's

---

[23] This observation is not a comment on the propriety of the search warrant for purposes of the Fourth Amendment or Article 1, Section 11 of the Indiana Constitution. We merely hold that for purposes of applying the foregone conclusion doctrine under the Fifth Amendment, the State has not described with reasonable particularity the digital files or data it seeks to compel.

[24] The dissent contends that, based on Detective Inglis's testimony at the hearing on the State's motion to hold Seo in contempt, "it seems self-evident the State is seeking evidence on Seo's phone of an App or multiple Apps that would allow her to mask her identity and evidence that Seo's phone had generated the phone calls and texts that D.S. received from phone numbers that did not belong to any other person." Slip op. at 65 n.8. But by the time Detective Inglis testified, the State had already obtained a warrant compelling Seo to unlock her phone. And there is nothing in the language of the warrant itself that describes with any particularity the information the State was authorized to look for. Although the dissent faults Seo for failing to present us with a more complete record, it is the language of the warrant itself, not the probable cause affidavit or testimony supporting the warrant, that is the controlling legal document which compels Seo to unlock her phone. And even after Detective Inglis's testimony, the order holding Seo in contempt again does not describe with any particularity the information the State seeks to compel.

name, rather than allowing the State to view everything that is contained in the messaging applications involved. These are not onerous requirements.

[54] Accordingly, we conclude that the State has not met the requirements of the foregone conclusion doctrine because it has not demonstrated that it can, with reasonable particularity, identify any files or describe where they are. *See Hubbell*, 530 U.S. at 45; *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1347; *Sec. & Exch. Comm'n*, 2015 WL 5611644 at *4. Instead, here, all the State has demonstrated is that evidence relating to the harassment and intimidation charges is probably on the phone. But it has failed to describe with adequate reasonable particularity the files or evidence it seeks on Seo's smartphone.

[55] It bears repeating that writs of assistance were the immediate evils that motivated the framing and adoption of the Fourth Amendment. *Payton v. New York*, 445 U.S. 573, 583 (1980). Although this case does not directly involve the Fourth Amendment, in criminal cases raising the Fifth Amendment, the law requires the State to describe the information it seeks to compel production of with reasonable particularity.

[56] Even in civil cases, modern, electronic discovery standards require that the requesting party specifically tailor its request to discover relevant information.

See Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322 (S.D.N.Y. 2003).[25] And in civil cases, opponents are also required to detail and attempt to obtain the information sought from third-party sources before seeking to compel the opponent to produce the information directly. The same should be true in criminal cases as well. Only then is an assault on Fifth Amendment privilege against self-incrimination a reasonable option under the law.

[57] As noted above, the Fifth Amendment privilege against self-incrimination reflects our nation's fundamental principles. These principles should not be altered by the advance of technology. To the contrary, they must be applied consistently and with recognition of the technology that has replaced physical papers, files, boxes and safes. *Cf. Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018) ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."); *Collins v. Virginia*, 138 S. Ct. 1663, 1671 (2018) (declining to expand the automobile exception to the warrant requirement to include a search of a vehicle parked in the curtilage of a home because to do so would "undervalue the core Fourth Amendment protection afforded to the home and its curtilage and 'untether' the automobile exception 'from the justifications underlying' it.") (quoting *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473, 2485 (2014)). Indeed, these principles

[25] In civil cases involving requests for discovery of electronic information, courts have applied a multi-factor test that includes consideration of the extent to which the request is specifically tailored to discover relevant information and the availability of such information from other sources. *Zubulake,* 217 F.R.D. at 322. Certainly, such concerns are all the more pressing in criminal cases where the State seeks production of digital information that may incriminate the defendant or others.

are all the more important given the amount and potentially incriminating nature of information contained in a smartphone.

VII. Outdated Analogies

[58] Advances in technology have rendered paper-based analogies more and more inapt, if not wholly inadequate. *See* Kiok, *supra* at 76 ("Many analogies to older technology simply do not replicate how electronic encryption actually works. Although metaphors are useful in analogizing new technology to older, more familiar one[s], if the metaphor is stretched too far, it loses its usefulness to courts and commentators."). Thus, to compare a smartphone and its contents to a paper file located in a locked file cabinet or wall safe, as the current case law does, is at the very least, a gross oversimplification. The information stored on a smartphone is qualitatively and quantitatively unique.

[59] As indicated in our introduction, the sheer quantity of personal information contained on a typical smartphone is truly astounding. In the years that the paper-based analogies were first made, it would have taken thousands, if not millions, of sheets of paper and photographs to equal the amount of digital information, such as email, text messages, photographs, and videos, stored in a modern smartphone.

[60] As recently as 2000, "only" 80 billion consumer photos were taken annually. Since the advent of the smartphone, this number has grown at an astonishing rate: by 2010, the number of photos taken annually had nearly tripled to over 200 billion, with projections that 1.3 *trillion* photos would be taken by 2017, and

over 79% of these photos were taken with some kind of phone. *See* Stephen Heyman, *Photos, Photos Everywhere*, N.Y. Times, July 29, 2015.[26] These predictions were pretty accurate, as it was reported that 1.2 trillion photos were taken in 2017, 85% taken with smartphones. *See* Caroline Cakebread, *People will take 1.2 trillion digital photos this year — thanks to smartphones*, Business Insider, Aug. 31, 2017.[27] A 2015 study revealed that the average smartphone user takes 150 photos per month and has 630 photos stored on the phone. *See* Janko Roettgers, *Special report: How we really use our camera phones*, GigaOm (Jan. 23, 2015, 5:00 a.m. CDT).[28] These numbers can only have grown since then with the increased storage capacity of more recent smartphones.

[61] Text messaging presents a similar story. A 2011 study by the Pew Research Center showed that users sent or received an average of 41.5 messages per day. *See* Aaron Smith, *How Americans Use Text Messaging,* Pew Research Center (Sept. 19, 2011).[29] This number has certainly only grown. Indeed, one report indicated that between 2011 and 2014, global text message usage grew by 140%. Kenneth Burke*, How Many Texts Do People Send Every Day?*, Text Request (May 18, 2016).[30] This same report indicates that globally 18.7 billion text

---

[26] *Available at* https://www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html

[27] http://www.businessinsider.com/12-trillion-photos-to-be-taken-in-2017-thanks-to-smartphones-chart-2017-8

[28] https://gigaom.com/2015/01/23/personal-photos-videos-user-generated-content-statistics/

[29] *Available at* http://www.pewinternet.org/2011/09/19/how-americans-use-text-messaging/

[30] https://www.textrequest.com/blog/how-many-texts-people-send-per-day/

messages were sent *every day*. *Id*. And these statistics do not include two of the most widely used app-to-app messaging platforms, WhatsApp and Facebook Messenger, which then combined for 60 billion messages per day. *Id*. Apple's Messages app sent over 40 billion notifications per day in 2016 and peaked at 200,000 messages per second. *See* Kif Leswing, *Apple says people send as many as 200,000 iMessages per second*, Business Insider, Feb. 13, 2016 (citing an interview of Apple Services Vice President Eddy Cue).[31]

[62] The point of these statistics is not to overwhelm the reader with numbers, but simply to illustrate how different a smartphone is from traditional paper-based media. To compare a smartphone to a locked strongbox or a wall safe, as the currently existing case law does, stretches these analogies beyond the breaking point. Perhaps a more apt analogy would be to compare a smartphone to a literal warehouse containing thousands of personal photographs, millions of lines of text contained in emails, messages, personal conversations, medical information, and other items of the most intimate nature. Some commentators have even compared a smartphone to a "second brain" or "an extension of the mind." *See* Yo Zushi, *Life with a smartphone is like having a second brain in your*

[31] http://www.businessinsider.com/eddy-cue-200k-imessages-per-second-2016-2 (citing *The Talk Show*, Daring Fireball (Feb. 12, 2016), https://daringfireball.net/thetalkshow/2016/02/12/ep-146

pocket, New Statesman (Feb. 22, 2017);[32] Karina Vold, *Is Your Smartphone an Extension of Your Mind?*, Motherboard (Mar. 2, 2018, 10:00 a.m.).[33]

[63] The paper-based analogies are also less and less apt as technology advances. In the days of the floppy disk, it was understandable to compare a digital file stored on such a disk to a physical piece of paper stored in a filing cabinet. Indeed, the basis of the most computer user interfaces retains the "desktop metaphor" of files, folders, and trash cans and recycling bins. But the advent of readily available, reliable, fast, and easy-to-use encryption has changed this metaphor. As noted above, encryption takes existing information and obscures it in such a manner that it is unreadable and unrecoverable unless it is decrypted with the proper key. To use the wall-safe metaphor, with encryption, when one locks the safe with the combination, the letter inside is shredded into millions of tiny pieces that no person could ever hope to reassemble; yet when one reenters the combination and unlocks the safe, the pieces of the letter almost magically reassemble themselves to reconstitute the letter.

[64] Despite the weaknesses of the current paper-based metaphors, the controlling Fifth Amendment case law still uses these metaphors. And we are not at liberty to create our own analogies or frameworks when it comes to the federal Constitution. This is a task reserved for the High Court itself. Thus, as we have explained, we believe that compelling an individual to unlock her smartphone

---

[32] https://www.newstatesman.com/science-tech/2017/02/life-smartphone-having-second-brain-your-pocket

[33] https://motherboard.vice.com/en_us/article/qvemgb/is-your-smartphone-an-extension-of-your-mind

by passcode is a testimonial act more akin to unlocking a wall safe than handing over the key to a locked strongbox.

VIII: A Way Forward?

[65] Electronic data storage of any type has stretched paper-based rules, rubrics, and rationales beyond their breaking points. As the *Fisher* court observed about the ruling in *Boyd* ninety years earlier, today, many paper-based rules, rubrics and rationales have not stood the test of time, especially as time is accelerated by developments in technology.[34] Simply said, electronic data and its storage are, by their nature, intrinsically different than records stored on paper, and the law must recognize that difference in order to honor our shared belief in a free society, limited only as reasonably required for public safety.[35] Going forward, we ask reviewing courts of last resort to consider the following structure for resolving decryption requests from law enforcement authorities:

---

[34] In 1965, American computer engineer Gordon Moore predicted that the number of transistors in a silicon chip would double every year. He later revised this prediction to a doubling of transistors every two years, but in reality, the pace has been a doubling every eighteen months. *See Moore's Law*, Encyclopædia Britannica (Nov. 29, 2017), *available at* https://www.britannica.com/technology/Moores-law. However, the laws of both physics and economics have recently brought the continuing validity of Moore's prediction into question. *See* Tom Simonite, *Moore's Law is Dead. Now What?*, MIT Technology Review (May 13, 2016), https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/; *End of Moore's Law: It's Not Just About Physics,* Scientific American (last visited Aug. 13, 2018), https://www.scientificamerican.com/article/end-of-moores-law-its-not-just-about-physics/.

[35] We must keep in mind that the Federalist Framers were forced to include a Bill of Rights, including the Fourth and Fifth Amendments, by their opponents, the Anti-Federalists, in the state ratification conventions. *See United States v. Emerson*, 270 F.3d 203, 237 (5th Cir. 2001) (noting that the Anti-Federalists wanted the United States Constitution, like most of the state Constitutions, to contain a Bill of Rights to prevent the federal government from infringing upon the fundamental rights of the people). Without the clear recognition of these personal rights, the United States, as we know it, would never have existed.

1. Requiring a defendant to decrypt digital data should be legally recognized for what it is—coerced recreation of incriminating evidence—and compulsory process for that purpose should be strictly limited for precisely that reason.

2. In some instances, law enforcement officials will have legitimate need of digital information that is protected by encryption.

3. If the law enforcement request is a *bona fide* emergency, with verified concern about the possibility of further and immediate serious criminal acts, a warrant that describes the other imminent crime(s) suspected and the relevant information sought through a warrant, both with reasonable particularity, will likely satisfy Fourth and Fifth Amendment requirements.

4. In non-emergency situations, law enforcement should be required to first seek the digital data it wants from third parties, such as internet "cloud" sources, cellphone companies, or internet providers (ISPs), where a defendant has practically, if not explicitly, consented to production upon legal process from a court of competent jurisdiction.[36]

5. Exceptions to the Fourth Amendment and its state analogues, such as the plain view doctrine and the good faith exception, should be

---

[36] Defendants in criminal cases are entitled to at least the same rights in this regard as are parties in civil cases. *See Zubulake*, 217 F.R.D. at 322.

inapplicable to, or strictly limited in, the search and seizure of digital data stored on devices owned or controlled by that defendant, or from "Cloud" subscriptions that defendant owns or uses. [37]

Conclusion

[66] Courts will continue to be faced with issues involving the intersection of the law and rapidly-emerging technology. Technology moves faster than the law. *See*, *e.g.*, *People v. Kramer*, 706 N.E.2d 731, 734 (N.Y. 1998). But the principles embodied in the Bill of Rights by our Founding Fathers are timeless. *See id*. ("[Technology] cannot be allowed to outpace the array of checks and balances and protections affecting [] privacy intrusions, important to individuals and society at large[.]").

[67] In this case, we apply these founding principles to modern technology and conclude that compelling Seo to unlock her iPhone, under the threat of contempt and imprisonment, is constitutionally prohibited by the Fifth Amendment because revealing or using the passcode to do so is a testimonial

---

[37] *See* Orin S. Kerr*, Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 314 (Jan. 2005) (suggesting that the plain view doctrine be abolished in computer searches because "computers often must be searched comprehensively to locate the evidence sought," and "the plain view rule threatens to collapse the distinction between particular and general warrants. A particular warrant in theory may become a general warrant in practice, as all of the evidence in the computer may come into plain view during the course of the forensic analysis."); Orin S. Kerr*, Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 576 (Apr. 2005) ("[A] tightening of the plain view doctrine may be necessary to ensure that computer warrants that are narrow in theory do not become broad in practice."); *see also* Orin S. Kerr*, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1, 21 (2015) (revisiting the author's earlier conclusions and suggesting that "[t]he plain view doctrine might not be the problem, and eliminating the plain view exception might not be the answer," and arguing that the use of non-responsive data found during a search instead renders the seizure unreasonable).

act. In addition, to date, the State has not met the requirements of the foregone conclusion doctrine: to describe with reasonable particularity the information it seeks to compel Seo to produce and why. In this non-emergency situation, the State should also first seek the evidence it feels it needs to prosecute the crime(s) alleged from third-party sources. We therefore reverse the order of the trial court finding Seo in contempt and remand for proceedings consistent with this opinion.[38]

[68] Reversed and remanded.

Riley, J., concurs in result.

May, J., dissents with opinion.

---

[38] As noted above, our opinion today does not foreclose the possibility of the State continuing the prosecution of Seo. *See* note 21, *supra*. Furthermore, the State may have other means of discovering the contents of Seo's phone. Although the contents of the phone itself are encrypted, some of the information might still be in the possession of third parties, such as the manufacturer of the phone (Apple, as to cellphone-number-spoofing apps downloaded by Seo) or her service provider (such as AT&T, Verizon, T-Mobile, Sprint, etc., as to when text messages were sent). And at least one manufacturer sells a turn-key solution that claims to be able to exploit an as-yet unrevealed vulnerability in the iPhone's passcode lockout feature to circumvent the lockout and enable police to brute-force the password. *See* Thomas Fox-Brewster, *Mysterious $15,000 'GrayKey' Promises To Unlock iPhone X For The Feds,* Forbes (March 5, 2018, 12:10 p.m.), https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/. However, a recently released update to the iPhone software apparently thwarts this exploit. *See* Chris Welch, *Apple releases iOS 11.4.1 and blocks passcode cracking tools used by police*, The Verge (July 9, 2018, 2:17 p.m.), https://www.theverge.com/2018/7/9/17549538/apple-ios-11-4-1-blocks-police-passcode-cracking-tools. This is all the more reason for courts to consider both smartphone users' privacy rights and the reasonable needs of law enforcement in a comprehensive way as soon as possible.

ATTORNEYS FOR APPELLANT

William J. Webster
Carla V. Garino
Webster Legal, LLC
Westfield, Indiana

ATTORNEYS FOR APPELLEE

Curtis T. Hill, Jr.
Attorney General of Indiana

Ellen H. Meilaender
Supervising Deputy Attorney General
Indianapolis, Indiana

IN THE COURT OF APPEALS OF INDIANA

Katelin Eunjoo Seo,
Appellant-Defendant,

v.

State of Indiana,
Appellee-Plaintiff.

Court of Appeals Case No.
29A05-1710-CR-2466

May, Judge, dissenting.

[69] When Seo wanted to have charges brought against D.S., she unlocked her cell phone and gave it to police so they could download its contents. Only by viewing those contents and then talking to D.S. did police learn that charges might instead be brought against Seo. Thus, the police already have proof that the cell phone in question belongs to Seo and that Seo can open it. Given that

those facts are a foregone conclusion, Seo's act of producing her unencrypted cell phone does not provide an inference of any "incriminating testimony" and, therefore, under the specific facts before us, I would hold Seo's Fifth Amendment right against self-incrimination is not being violated by the order that she unlock the phone. *See*, *e.g.*, *United States v. Spencer*, 2018 WL 1964588 (N.D. Cal. 2018) (Fifth Amendment not violated by order for Spencer to decrypt the device where the State demonstrated, by clear and convincing evidence, that Spencer's ability to decrypt the device is a foregone conclusion). Accordingly, I respectfully dissent.

[70] To explain why I reach that conclusion and where my understanding of Fifth Amendment jurisprudence diverges from the majority's opinion, I need to address numerous parts of the majority's analysis.

Privacy and the Fifth Amendment

[71] As the majority notes, modern Fifth Amendment jurisprudence begins with *Boyd v. United States*, 116 U.S. 616 (1886). *Slip op*. at 15 (discussing *Boyd*). *See also* Wayne R. LaFave, Jerold H. Israel, Nancy J. King, & Orin S. Kerr, *Criminal Procedure: The Boyd "principle"*, *in* 3 CRIM. PROC. § 8.12(a) (4th ed., Dec. 2017 Update) (hereinafter "LaFave et al., *Boyd principle*") ("the *Boyd* analysis remains a universally accepted starting point for understanding the many strands of current Fifth Amendment doctrine applicable to the *subpoena duces tecum*"). *Boyd* held "the seizure of a man's private books and papers to be used in evidence against him is [not] substantially different from compelling

him to be a witness against himself." *Boyd*, 116 U.S. at 633. As LaFave and his colleagues explain:

> *Boyd* relied on what has been described as a "property oriented" view of the Fourth and Fifth Amendments, built upon the owner's right of privacy in the control of his lawfully held possessions. It recognized a special Fifth Amendment interest in the privacy of documents, viewing the forced production of their contents as equivalent to requiring a subpoenaed party to reveal that content through his testimony. . . . [T]he key to the Court's analysis appeared to be invasion through forced production of the individual's privacy interest in his possession of property in which the public had no entitlement.

LaFave et al., *Boyd principle*.

[72] Since that time, however, the Supreme Court has "gradually developed a series of doctrines that chipped away at the broad implications of *Boyd*'s property-rights/privacy analysis of Fifth Amendment protection," *id.*, such that "very little if anything, remains of *Boyd*'s Fifth Amendment analysis." *Id*. *See also Carpenter v. United States*, 2018 WL 3073916 at *66 (2018) (Gorsuch, J., dissenting) ("To be sure, we must be wary of returning to the doctrine of *Boyd* . . . [which] invoked the Fourth Amendment to restrict the use of subpoenas even for ordinary business records and, as Justice Alito notes, eventually proved unworkable."). In fact, in 1976, the Supreme Court explicitly rejected the idea that the Fifth Amendment was intended to protect private information:

> The proposition that the Fifth Amendment protects private information obtained without compelling self-incriminating testimony is contrary to the clear statements of this Court that

> under appropriate safeguards private incriminating statements of an accused may be overheard and used in evidence, if they are not compelled at the time they were uttered; and that disclosure of private information may be compelled if immunity removes the risk of incrimination. If the Fifth Amendment protected generally against the obtaining of private information from a man's mouth or pen or house, its protections would presumably not be lifted by probable cause and a warrant or by immunity. The privacy invasion is not mitigated by immunity; and the Fifth Amendment's strictures, unlike the Fourth's, are not removed by showing reasonableness. The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination.
>
> We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against "compelled self-incrimination, not (the disclosure of) private information."

Fisher v. United States, 425 U.S. 391, 400-01 (1976). *See also* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. Rev. Discourse 298, 307 (2014) ("Privacy is no longer a Fifth Amendment value.").

[73] Because the United States Supreme Court has explicitly rejected the notion that the Fifth Amendment is intended to protect any privacy interest in information, I find irrelevant my colleagues' repeated references to the "trove of . . . almost

always embarrassing, and potentially, incriminating" information they keep on their cell phones. *Slip op*. at 2-3; *see also id*. at 1-2 ("The amount of personal information contained on a typical smartphone is astounding[.]"); *id*. at 26 n.20 ("[G]iven the vast amounts of personal information located on a typical smartphone, there should be a reasonable presumption that *something* incriminating would be discovered during review of the contents of almost anyone's smartphone.") (emphasis in original);[39] and *id*. at 36-38 (discussing the amount of data processed by and kept on phones).

Encryption and Its Implications

[74] Part of the reasoning behind the majority's holding that forcing Seo to unlock her phone implicates the Fifth Amendment is because

> her act of unlocking, and thereby decrypting, her phone effectively recreates the files sought by the State. . . . In a very real sense, the files do not exist on the phone in any meaningful way until the passcode is entered and the files sought are decrypted.

[39] In the same footnote, my colleagues express concern about "the expansive law enforcement claims that could be made under the plain view doctrine or the good faith exception to the Fourth Amendment or Article 1 Section 11 of the Constitution of Indiana protections when searching a smartphone." *Slip op*. at 26 n.20. While I am not unconcerned about the implications of plain view and good faith when the police are given unfettered access to the contents of a citizen's smartphone, I also recognize that the application of the Fourth Amendment is not before us in this appeal and that our decision under the Fifth Amendment ought not be conflated with Fourth Amendment concerns. *See Carpenter*, 2018 WL 3073916 at *13 ("Our decision today is a narrow one. We do not express a view on matters not before us."); *and see Fisher*, 425 U.S. at 401 ("the Fifth Amendment protects against 'compelled self-incrimination, not (the disclosure of) private information'").

Slip op. at 25. I concede that encryption turns readable digital data into digital random noise. I cannot, however, agree that decryption constitutes "creation of testimony" that should implicate the Fifth Amendment.

[75] Seo is not being forced, under the penalties of perjury or torture, to download new Apps or to write and send new text messages. The evidence being sought from Seo's phone – text messages matching those received by D.S. from phone numbers that were not assigned to any identifiable person and identity masking applications – already are among the files on Seo's phone, otherwise they could not have been encrypted when Seo locked her phone.[40] As such, decryption does not use the contents of Seo's mind to create *new* information. Instead, pre-existing information is simply being rendered intelligible.

[76] Therefore, in my opinion, the law ought to treat files on a cell phone – encrypted or not – like prior-produced documents sitting in a file cabinet, which do not enjoy Fifth Amendment protection. *See United States v. Hubbell*, 530 U.S. 27, 35-36 (2000) ("a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege"); *id*. at 36 ("Hubbell could not avoid compliance with the subpoena served on him merely because the demanded documents contained incriminating evidence, whether written by others or voluntarily prepared by

---

[40] The question of whether the State has probable cause to believe it will find that expected evidence of the alleged crimes on Seo's phone is a Fourth Amendment question that, once again, is not before us in this appeal. *See supra* n. 39. Accordingly, for my analysis, I assume *arguendo* the evidence exists on her phone.

himself."); *Fisher*, 425 U.S. at 409-410 ("the preparation of all of the papers sought in these cases was wholly voluntary, and they cannot be said to contain compelled testimonial evidence, either of the taxpayers or of anyone else"). *See also In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1342 (11th Cir. 2012) ("the files, if there are any at all in the hidden portions of the hard drives, are not themselves testimonial").

[77] To hold otherwise as to data on encrypted devices creates an ever-increasingly unpoliceable "zone of lawlessness" that could not have been envisioned when the Fifth Amendment was adopted. *See* Dan Terzian, *The Micro-Hornbook on the Fifth Amendment and Encryption*, 104 Geo. L.J. Online 168 (2016) ("The DOJ calls encryption a "zone of lawlessness."); *see also Slip op.* at 12 (advanced security features on modern cellphones render nearly impossible brute force attacks on passcodes, such that "if the police want or need to gain access to an iPhone, the cooperation of its owner is practically a necessity"). The Fifth Amendment, like other portions of the Bill of Rights, was intended to balance the government's interest in policing to maintain the common welfare of the people with each individual citizen's interest in liberty from government intrusion. *See California v. Byers*, 402 U.S. 424, 427 (1971) (Fifth Amendment questions "must be resolved in terms of balancing the public need on the one hand, and the individual claim to constitutional protections on the other; neither interest can be treated lightly."); *see also* Terzian, 61 UCLA L. Rev. Discourse *at* 307 ("Forming the Fifth Amendment's core value, then, is its aim to achieve a fair state-individual balance. Where there is a real societal need to

limit the privilege, the Court has repeatedly permitted compulsion upon the defendant."). I do not believe the creation of a zone-of-lawlessness outside a person's mind from which individual citizens could commit crimes against others without government recourse can be a proper balancing of those interests. *See generally id*. Accordingly, I believe we must find a path forward that balances the governmental and individual interests without creating a zone of lawlessness from which one citizen may harass another without government intervention. *See*, *e.g.*, *Kastigar v. United States*, 406 U.S. 441, 445-46 (1972) (statutes granting immunity for compelled testimony "seek a rational accommodation between the imperatives of the privilege and the legitimate demands of government to compel citizens to testify"), *reh'g denied*.

Keys, Combinations, and the "Contents of One's Mind"

[78] As the majority discusses, in 1988, the United States Supreme Court decided a citizen's Fifth Amendment privilege against self-incrimination was not violated by an order that compelled him to sign a consent form authorizing foreign banks to release any records of accounts in his name to the United States government. *Doe v. United States*, 487 U.S. 201, 219 (1988) (hereinafter "*Doe 2*"). Justice Stevens dissented from that decision, arguing that a citizen "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 by deed." *Id*. at 219 (Stevens, J., dissenting). In response, the Court's majority noted:

> We do not disagree with the dissent that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. In our view, such compulsion is 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.

[79] A majority of the Supreme Court again referenced this key-combination dichotomy when it decided *Hubbell*:

> It was 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. 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.

Hubbell, 530 U.S. at 43 (Hubbell's Fifth Amendment privilege was violated by a subpoena that forced him to comb through thousands of documents to find those that fit the government's request.).

[80] Based on that language from *Doe 2* and *Hubbell*, courts being asked to determine whether a citizen could be forced to reveal the passcode for locked electronic devices have frequently turned to this key-combination dichotomy and asked whether the electronic passcode is more like a key or a combination. Some courts have held that a passcode is more like a combination because both are

kept in a person's mind, such that the production of the password would be testimonial and is prohibited by the Fifth Amendment.[41] *See*, *e.g.*, *United States v. Kirschner*, 823 F.Supp. 2d 665, 668-9 (E.D. Mich. 2010) (government cannot compel disclosure of password because it requires defendant "to divulge through his mental processes his password"); *In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473, at *4 (D. Vt. Nov. 28, 2007) ("A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena.") (hereinafter "*Boucher 1*", *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb 19, 2009) (enforcing subpoena seeking decrypted data, but not the password itself) (hereinafter "*Boucher 2*").

[81] However, at least one commentator on Fifth Amendment jurisprudence argues courts ought to reconsider whether to apply this key-combination dichotomy to electronic passcodes:

> Passwords should not be forced into this key-combination dichotomy. They are neither a key nor a combination, and Court doctrine suggests the dichotomy should not be mechanically applied to new unlocking mechanisms. This dichotomy developed because keys and combinations have different Fifth Amendment implications—only combinations present the danger of compelling the creation of evidence. So it follows that new unlocking mechanisms with new implications should also be treated differently. Passwords for encrypted data present new

[41] If, however, the passcode were written down on a piece of paper and placed in a drawer, then production of that passcode undoubtedly could be compelled because in those circumstances the passcode is indistinguishable from a key. Terzian, 104 Geo. L.J. Online at 169 n.8 (noting "if the password is physically recorded somewhere, the government can subpoena the production of that password" but "the subpoena won't yield anything if (when) the defendant responds that there is no written password").

> implications in interest balancing and therefore should be treated differently. First, consider the interest balancing with safe combinations. There, a fair state-individual balance favors the individual—and compelled production is prohibited—because there is little state need; law enforcement can easily crack a safe through its own efforts. Contrast that with passwords. Law enforcement usually cannot bypass them, leaving the data inaccessible and creating great need for the password or decrypted data's production.

Terzian, 61 UCLA L. Rev. Discourse at 301-2.

[82] Others have challenged the logic of applying this key-combination dichotomy because the government's ability to open an electronic device should not be determined by "whether [someone] protected that drive using a fingerprint key or a password composed of symbols." *Spencer*, 2018 WL 1964588 at *2. *See also State v. Stahl*, 206 So.3d 124, 135 (Fla. Ct. App. 2016) ("we are not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint as the passcode"). As the majority notes, there is little doubt that the government could compel a citizen to display a physical characteristic, even if that characteristic might be incriminating, because it is not testimonial. *Slip op*. at 14 n.14.[42] Thus, arguably, courts could compel citizens to open an electronic device that is

[42] The majority then asserts this reasoning is "outdated and ironic when compared with" modern electronic scanning mechanisms. *Slip op.* at 14 n.14. The majority does not explain how or why advanced scanning equipment should lead courts to overturn the long-standing rule that physical characteristics are not testimony, and I thus cannot agree with the majority that this rule is "outdated and ironic." *Id.*

unlocked by fingerprint, retinal scan, or face scan, because production of those physical characteristics is not "testimony" prohibited by the Fifth Amendment. *See Schmerber v. California*, 384 U.S. 757, 764 (1966) (physical evidence can be compelled and Fifth Amendment does not protect against the compulsion to provide fingerprints); *Hubbell*, 530 U.S. at 34-5 ("[E]ven though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice.") (footnotes omitted); *United States v. Hook*, 471 F.3d 766, 773-74 (7th Cir. 2006) ("[T]he taking of blood samples or fingerprints is not testimonial evidence and as such is not protected by the Fifth Amendment."), *cert. denied*. 549 U.S. 1343.

[83] The majority herein decides: "under the precedent as it now exists, we hold that the State is seeking the electronic equivalent to a combination to a wall safe—the passcode to unlock the iPhone." *Slip op.* at 22. I do not believe the precedent compels the result the majority reaches, because while a passcode is similar to a combination, an electronic device arguably is materially distinguishable from a wall safe. Nor do I believe the majority ought to be deciding an issue that is not before us today, as Seo has not been asked to reveal her password. *See Carpenter*, 2018 WL 3073916 at *13 ("Our decision today is a narrow one. We do not express a view on matters not before us. . . . As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'"). I accordingly dissent from the majority's

unnecessarily holding a passcode is the equivalent of a combination to a wall safe.

[84] The trial court instead ordered Seo to produce the decrypted device. The Eleventh Circuit considered whether forced decryption was testimonial and determined it too was compelled testimony prohibited by the Fifth Amendment because "the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346.

[85] This Eleventh Circuit holding has been challenged on two grounds:

> First, it misreads Supreme Court dicta. The dicta regards only compelling production: The government can compel the production of keys but not the production of combinations. It's silent on whether the government can compel unlocking (i.e., forcing a person to enter a combination without producing a copy). This silence, coupled with the dicta's rationale, suggests that compelling unlocking may be constitutional. The reason for the Court distinguishing between key- and combination-productions stems from the Court's concern over compelled creation. Combinations may not exist outside a person's mind, so producing them would require compelling the creation of a physical version, and it is this compelled creation that makes the response testimonial. There are no such compelled creation concerns with compelled unlocking through forced decryption—the data is already there, the person just needs to unlock it; and unlocking it does not require creating a physical copy of the password.

> The second stumble comes in the Eleventh Circuit's analysis of mental effort. Entering an oft-used password requires no more mental effort than finding a key. You remember the key's location and then find it, just as you remember the password and then input it.

Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How Riley Matters*, 109 Nw. U. L. Rev. Online 56, 59-60 (2014).[43]

[86] The majority herein explicitly rejects the State's attempt to distinguish production of the passcode from production of the unlocked device "because the end result is the same: the State is compelling Seo to divulge the contents of her mind." *Slip op*. at 25. By so holding, the majority has fallen into the first "stumble" noted above – Seo is not being required to "divulge" anything from her mind. Just the opposite, she is unlocking the device *without* revealing the contents of her mind, and to the extent she is required to use her mind to do so, the mental effort is no greater than the mental effort required to locate and

---

[43] Elsewhere, Terzian objected to the Eleventh Circuit's decision thus:

> [The Eleventh Circuit] addressed the question of whether the Fifth Amendment bars the compelled decryption and production of the now-unencrypted data. It held affirmatively and explicitly framed the issue within this dichotomy, finding compelled decryption "most certainly more akin to requiring the production of a combination."
>
> This reasoning ignores a pivotal prefatory question: Do passwords even belong in this dichotomy? A computer password is not a safe combination. Sure, they are similar, but that does not mean they *must* be treated the same. Combinations and keys are similar—both unlock safes—yet they are treated differently because only the former implicated compelled creation concerns.
>
> It follows, then, that courts should treat passwords and combinations differently if they have meaningfully different Fifth Amendment implications. And they do. Passwords and encrypted data implicate fair balancing concerns that support permitting compelled production, while combinations do not.

Terzian, 61 UCLA L. Rev. Discourse at 306.

produce a key to a file cabinet. For these reasons, I would hold the only self-incrimination ground for challenging the compelled production of an unlocked and decrypted electronic device "lies in the testimonial aspects of the act-of-production," just as it does with the production of preexisting papers. Wayne R. LaFave, Jerold H. Israel, Nancy J. King, & Orin S. Scott, *The Schmerber rule*, 3 CRIM. PROC. § 8.12(d) n.48 (4th ed. Dec. 2017 Update) (hereinafter "LaFave et al., *Schmerber rule*"). And it is to this issue that I turn next.

Act of Production, Foregone Conclusion, & Reasonable Specificity

[87] The act of producing a decrypted device might itself be protected by the Fifth Amendment. *See Hubbell*, 530 U.S. at 37 ("Whether the constitutional privilege protects . . . the act of production itself . . . is a question that is distinct from the question whether the unprotected contents of the documents themselves are incriminating."). To explain why I do not believe Seo's production of her decrypted iPhone implicates Fifth Amendment concerns, I begin with a discussion of the relevant case law.

[88] Our country's Highest Court explained:

> The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It would also indicate the taxpayer's belief that the papers are those described in the subpoena. The elements of compulsion are clearly present, but the more difficult issues are whether the tacit averments of the taxpayer are both "testimonial" and "incriminating" for

> purposes of applying the Fifth Amendment. These questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof.

Fisher, 425 U.S. at 410 (internal citation omitted).

[89] In *Fisher*, the government subpoenaed tax preparation documents that had been produced by an accountant and were in the accountant's files. The Court noted the Fifth Amendment did not apply to the documents themselves "because the documents were created voluntarily and the Government had not compelled their creation." Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. Pub. Int. L.J. 53, 61 (Winter 2015) (citing *Fisher*, 425 U.S. at 410 n.11). The *Fisher* Court determined "the act of producing [the papers] would not itself involve testimonial self-incrimination." 425 U.S. at 411.

> The 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. Surely the Government is in no way relying on the "truth-telling" of the taxpayer to prove the existence of or his access to the documents. The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender."

Id. (internal citations omitted).

[90] That holding by the *Fisher* Court created what has become known as the foregone conclusion standard, which has been described thus:

> Where the existence and possession of the documents to be produced are a "foregone conclusion," the act of production similarly "adds little or nothing to the sum total of the government's information" and therefore is no more testimonial than other compelled physical acts. The government in such a case obviously is not seeking the assertions of the subpoenaed party as to the facts of existence and possession, and his incidental communication as to those facts, inherent in the physical act that the government had the authority to compel, therefore does not rise to the level of compelled "testimony."

Wayne R. LaFave, Jerold H. Israel, Nancy J. King, & Orin S. Kerr, *Testimonial character and the foregone conclusion standard*, 3 CRIM. PROC. § 8.13(a) (4th ed. Dec. 2017 Update) (hereinafter "LaFave et al., *Foregone Conclusion*").

[91] In *United States v. Doe*, 465 U.S. 605, 613 (1984) (hereinafter, "*Doe 1*"), the Supreme Court was again asked to decide whether the act of producing documents would violate a citizen's Fifth Amendment right. The District Court had found "enforcement of the subpoenas would compel [respondent] to admit that the records exist, that they are in his possession, and that they are authentic." *Id*. at 613 n.11. The Supreme Court noted it could "not over turn that finding unless it has no support in the record." *Id*. at 614. Based thereon, the Supreme Court held Doe's act of producing the subpoenaed documents to be protected by the Fifth Amendment privilege against self-incrimination. *Id*. at 614.

> Subsequent to *Doe [1]*, lower court rulings generally insisted that the foregone conclusion standard be met by the government "demonstrat[ing] with reasonable particularity that it knows of the existence and location of subpoenaed documents." Those rulings recognized, however, that there are a variety of ways in which such a demonstration may be made. These include: some prior action by the subpoenaed party acknowledging that the particular documents existed and were in his possession; identification of some person (as in the case of the accountants in *Fisher*) who can testify that the particular documents were previously in the possession of the subpoenaed party; documents or similar evidence in the government's possession which would indicate that the subpoenaed documents exist and are in the subpoenaed person's possession; and the fact that the documents are of a type regularly sent to the subpoenaed person by another doing business with that person, combined with absence of any dispute as to whether he received such documents. Similarly, as to authentication, courts held that the foregone conclusion standard is met where the government can point to another person (e.g., the preparer of the document) who can authenticate, or where authentication can be achieved by other means (e.g., comparison with other documents independently authenticated or matching the handwriting with that of the subpoenaed party). As with existence and possession, the government must point to a specific avenue of authentication "by means independent of the producer's act of production. To merely state that [the government] will not utilize the act of production would amount to no more than an informal offer of immunity, which *Doe [1]* rejected as an inappropriate grounding for enforcing the subpoena.

LaFave et al., *Foregone Conclusion* (footnotes omitted).

[92] Then, in *Hubbell*, the Supreme Court was asked to decide "whether the Fifth Amendment privilege protects a witness from being compelled to disclose the

existence of incriminating documents that the Government is unable to describe with reasonable particularity[.]" *Hubbell,* 530 U.S. at 29-30 (footnote omitted). There, the governments subpoenaed eleven categories of documents from a grand jury witness, Hubbell. Hubbell invoked his Fifth Amendment privilege and refused to admit whether he had such documents. The prosecutor then promised Hubbell immunity, and Hubbell produced 13,120 pages of documents and testified those were all the documents in his control that were requested by the subpoena.[44] *Id*. at 31. Based on the information in those documents, the government brought a second set of charges against Hubbell for crimes the government had not been investigating when Hubbell responded to the subpoena. Instead, the government had discovered those crimes by studying the contents of the documents Hubbell produced. *Id*. at 32.

[93] The Supreme Court noted:

> [W]hen the custodian of documents responds to a subpoena, he may be compelled to take the witness stand and answer questions designed to determine whether he has produced everything demanded by the subpoena. The answers to those questions, as well as the act of production itself, may certainly communicate information about the existence, custody, and authenticity of the documents.

[44] All, that is, except those protected by attorney-client privilege or work-product privilege. *Hubbell*, 530 U.S. at 31.

Id. at 37. The Court then held Hubbell's act of production had a testimonial aspect because the government had not demonstrated the testimony produced was a foregone conclusion:

> Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it. While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent.

Id. at 44-45.

[94] Because *Hubbell* did not clarify the scope of the foregone conclusion standard, lower courts have continued to struggle with determining whether an act of production is both testimonial and incriminating based "on the facts and circumstances of particular cases." *Fisher*, 425 U.S. at 410. Courts have especially had difficulty when applying this standard to compulsory decryption of an electronic device, "often reconsidering and overturning their own prior orders when faced with changing facts, or facts that were not well-understood in the first place." Kiok, 24 B.U. Pub. Int. L.J. at 65.

[95] The majority's review of the parties' arguments provides citation to many of these cases, with parentheticals describing the various holdings, so I need not repeat all of them here. *See Slip op*. at 29-31. Instead, I provide this summary:

> A defendant's ability to invoke the Fifth Amendment in the context of a compulsory order to decrypt will depend on the foregone conclusion doctrine and events that in all likelihood long preceded the subpoena or warrant. The foregone conclusion doctrine will permit the Government to compel a defendant when the Government can otherwise prove that the hard drive and its data was the sole property of the defendant. If a defendant confesses to possession of the drive, that may suffice. If the Government can view some portion of the hard drive and determine that the files belonged to one individual, that too may suffice.

Kiok, 24 B.U. Pub. Int. L.J at 77-78 (footnotes omitted).

[96] Herein, the majority holds that

> what the State seeks to compel is not merely the password, but the entire contents of Seo's iPhone. Thus, for the foregone conclusion rationale to apply, the State must be able to describe with reasonable particularity the *discrete* contents on Seo's phone—e.g., all texts to D.S. created on Seo's iPhone—that it is compelling her to not only produce, but to re-create by entering her passcode and decrypting the contents of the phone. This is a burden the State has not met.

Slip op. at 31 (emphasis in original).

[97] However, in so holding, the majority has followed authority that, I believe, misapplies the foregone conclusion doctrine to electronic devices.[45] The State

[45] In addition, the majority's holding relies on a premise that I do not accept – that the contents of a decrypted electronic device are the equivalent of testimony created by compulsion. *See supra* **Encryption and Its Implications**.

has not presented Seo with a subpoena requiring her to produce each text message she sent to D.S., such that Seo must, like Hubbell, use her mind to discern which text messages fit within the categories of messages requested and then testify that she produced all relevant requested evidence. *See Hubbell*, 530 U.S. at 45 ("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"). Nor has Seo been ordered to sort through thousands of electronic devices in her possession to produce those devices that contain the requested evidence.

[98] Instead, the State has asked Seo to unlock a file cabinet so that the State may search within that file cabinet for evidence of specific crimes the State is already investigating. The State's right to access such a file cabinet will undoubtedly require a Fourth Amendment showing of probable cause to believe the particular evidence sought will exist within that cabinet. *See* U.S. Const. amend. IV ("no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"). But the validity under the Fourth Amendment of the order for Seo to open her phone is not before us, and the Fifth Amendment does not require the State to demonstrate in advance "the *discrete* contents" of the evidence that will be found in a cabinet,[46] *see United*

[46] Even if I could agree with my colleagues that the reasonable particularity standard required the State to make a showing, with reasonable particularity, of the evidence it expects to find within the electronic device being sought, I would be hesitant to hold, based on the record before us, that the State had not met that

States v. Fricosu, 841 F.Supp.2d 1232, 1237 (D. Col. 2012) ("[T]he government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production[.]"), because the Fifth Amendment does not protect the content of the documents. *See Fisher*, 425 U.S. at 409 ("the Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications").

---

standard herein. At the hearing on the State's motion for rule to show cause, Detective Inglis testified that Seo initially used her own phone number to contact D.S.; however,

> [t]hen the contact to [D.S.] started coming from more random phone numbers that when I would try and research the phone number to find out who it belonged to, or who it was assigned to, there was no record of it being assigned to anybody and the numbers would change. He would get a dozen or 30 phone calls or texts from one number and then the next day it would be a different number but it would obviously be conversations that were linked with the same.

(Tr. at 7.) D.S. was contacted by "dozens of phone numbers." (*Id.*) Detective Inglis said "it appeared that she was using an ap [sic] or an internet program such as Google Voice or Pinger to disguise her phone number so that it wouldn't show up in his caller ID." (*Id.* at 8.) The State asked Detective Inglis if he had subpoenaed the Apps or Internet services that could mask identity, and he testified:

> There are numerous, and there's probably some that I'm not even aware of, numerous entities out there like Google Voice and Pinger and Text Now and Text Me, and I don't know, I don't have an all-encompassing list of them, however if I had the phone I could see which ones she had accessed.

(Tr. at 12.) Thus, it seems self-evident the State is seeking evidence on Seo's phone of an App or multiple Apps that would allow her to mask her identity and evidence that Seo's phone had generated the phone calls and texts that D.S. received from phone numbers that did not belong to any other person.

Also troubling for me is the majority's insistence "the State has not described with reasonable particularity the digital files or data it seeks to compel," (*Slip op.* at 33 n.25; *and see id.* at 32), when the Record provided to us on Appeal does not contain any of the documentation or testimony provided to the trial court before the search warrant was issued. I acknowledge "the warrant itself does not describe with any particularity the digital information the State seeks to compel," (*id.* at 33), but I would not infer from the absence of such description in the warrant that the evidence is likewise absent from portions of the Record that Seo has not provided to us.

[99] Because of this material distinction between the order in *Hubbell* and this order to open an iPhone, the only testimony being implied by Seo's act of decrypting the phone is that the phone is hers and she has the ability to unlock it.[47] These are facts the State can already prove by "clear and convincing evidence," *Spencer*, 2018 WL 1964588 at *3 ("The appropriate standard is instead clear and convincing evidence. This places a high burden on the government to demonstrate that the defendant's ability to decrypt the device at issue is a foregone conclusion."), because Seo has already unlocked the phone for police when she gave it to them to download, the investigating officer had called Seo at the phone number associated with the phone in question, and Seo admitted the phone was hers when she was arrested. As such, Seo's act of production does "not itself involve testimonial self-incrimination." *Fisher*, 425 U.S. at 411; *see Spencer*, 2018 WL 1964588 (foregone conclusion applies where defendant admitted buying and encrypting external hard drive matching one found in his house); *Friscosu*, 841 F. Supp. 2d at 1236-37 (foregone conclusion applies where State knows computer belongs to defendant and knows she has password).

In Summary

[100] The Fifth Amendment is intended to prohibit the government from compelling incriminating testimony, not to protect the privacy of personal information. The Fifth Amendment could not have been intended to create a zone-of-

[47] Moreover, it is unnecessary to "ask whether the government has established with 'reasonable particularity' that the defendant is able to decrypt a device. . . . [A] defendant's ability to decrypt is not subject to the same sliding scale. He is either able to do so, or he is not." *Spencer*, 2018 WL 1964588 at *3.

lawlessness outside a person's mind that the government would be unable to police to maintain the safety of all citizens. While decrypting an electronic device requires the use of the contents of the owner's mind, the task requires such little mental effort that I would hold the only Fifth Amendment barrier to production of the decrypted device is if the act of production itself implies incriminating testimony. The act of production cannot, however, produce incriminating testimony when the facts confirmed by that decryption – that the citizen owns the device and has the ability to decrypt it – are a foregone conclusion because the government already has clear and convincing evidence of those facts.

[101] As Seo unlocked her phone for police on another occasion, as police had contacted Seo on that phone, and as Seo admitted the phone was hers when she was arrested, I would hold Seo's possession and ability to decrypt the phone are foregone conclusions. Seo therefore can be compelled to decrypt her phone without infringing the Fifth Amendment.

[102] For all these reasons, I respectfully dissent.