Filed: 2/28/2019 6:48 PM

IN THE
INDIANA SUPREME COURT
CASE NO. 18S-CR-595

Katelin Eunjoo Seo, Appellant,	)	Appeal from the Hamilton Superior Court 1
v.	)	Trial Court Case No. 29D01–1708–MC–5640
State of Indiana, Appellee.	)	The Honorable Steven R. Nation, Judge

APPELLANT'S RESPONSE TO BRIEF OF AMICUS CURIAE STATES OF UTAH, GEORGIA, IDAHO, LOUISIANA, MONTANA, NEBRASKA, OKLAHOMA, AND PENNSYLVANIA

William J. Webster, Atty No. 29086-29
WEBSTER & GARINO LLC
104 N. Union St.
Westfield, IN 46074
Phone: (317) 565-1818

Attorney for Appellant Katelin Eunjoo Seo

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

I.

SUMMARY OF THE ARGUMENT

In this case, the State of Indiana seeks to compel Katelyn Eunjoo Seo ("Seo") to unlock her cell phone, an IPhone 7, through her recollection and use of a memorized password without any limitation to search for incriminating evidence.

II.

BRIEF STATEMENT OF THE CASE

The State of Indiana obtained a search warrant, which provided in part that Seo be compelled to unlock her I Phone 7 via biometric fingerprint, passcode, password or otherwise. Seo declined to provide her password to investigators citing her right against self-incrimination under the Fifth Amendment of the United States Constitution. The State filed a motion for contempt for Seo's refusal to unlock her phone. The Trial Court found Seo in contempt and ordered Seo to be incarcerated until she unlocked her cell phone. Upon appeal, the Indiana Court of Appeals reversed the Trial Court, finding that the trial court's Order compelling Seo to unlock her phone violated her guarantee against self-incrimination under the Fifth Amendment to the United State Constitution. *See* K*atelin Eunjoo Seo v. State of Indiana,* 29A05-1710-CR-2466 (Ind. Ct. App.2018). The State of Indiana appealed the decision made by the Court of Appeals and eight (8) states, Utah, Georgia, Idaho, Louisiana, Montana, Nebraska, Oklahoma, and Pennsylvania, have joined to file an amicus brief in support of the State ("States' Brief").

III.

AMICUS STATES' ARGUMENT

The States' Brief primarily consists of policy arguments, assumptions and hypotheticals that suggest if the Indiana Supreme Court affirms the decision of the Indiana Court of Appeals,

States will be incapable of executing search warrants and obtaining evidence, a new zone of lawlessness will be created where child pornographers and drug dealers can operate without fear of law enforcement, and the public will want and encourage lawmakers to pass new draconian anti-privacy legislation. Even though encryption is fairly new in our society, the frustration articulated by the States is not: investigators believe additional evidence of a crime exists and the person investigators believe has the knowledge necessary to obtain that evidence is the criminal suspect. Decades if not centuries of precedent and practice support the conclusion that a suspect cannot be compelled to recall and use information that exists only in his or her mind in order to aid the government's prosecution. *See Curcio v. United States*, 354 US 118, 128 (1957). Absent a grant of immunity that compulsion violates the Fifth Amendment privilege against self-incrimination. Counsel recognizes the challenges law enforcement agencies face in criminal investigations and the important role they play in our society. However, the Fifth Amendment should not be viewed as an inconvenience to law enforcement. The Court's focus should be on the zone of liberty the Fifth Amendment affords -- not the hypothetical zone of lawlessness the States propose the Fifth Amendment creates. This guarantee against testimonial compulsion, like other provisions of the Bill of Rights, "was added to the original Constitution in the conviction that too high a price may be paid even for the unhampered enforcement of the criminal law and that, in its attainment, other social objects of a free society should not be sacrificed." See *Feldman v. United States*, 322, U. S. 487, 489 (1944). This provision of the Amendment must be accorded liberal construction in favor of the right it was intended to secure. See *Counselman v. Hitchcock*, 142 U.S. 547, 562 (1892); *Arndstein v. McCarthy*, 254 U.S. 71, 72-73 (1920).

The policy arguments presented by the States should not be grounds to reverse the decision made by the Indiana Court of Appeals, as explained in more depth below.

Response to Brief of Amicus Curiae, States of Utah, Georgia, Idaho, Louisiana, Montana, Nebraska, Oklahoma, and Pennsylvania

A. Modern encryption does not place nearly unbreakable locks on digital information.

The States frame the term and use of "encryption" as something secretive or concealing, suggesting that someone who uses encryption does so for the nefarious purpose of concealing the true meaning of a message. The States go so far as pointing out that the word encryption is based in part from the Greek word meaning "secret writing." *See* Brief of Amici Curiae State of Utah et al, p. 7-8. The States suggest that it is "essentially impossible for even the most powerful computers to break a digital lock by current brute force techniques that try every combination." *Id*. p. 10. In reviewing the States' explanation of encryption, one may come to the opinion that encryption is a tool only reserved for criminal enterprises. Further, in making their argument, the States rely on articles written by Orin S. Kerr, who is a former federal computer crimes investigator. However, encryption is integral for safeguarding the privacy and security of sensitive, electronically stored information. The use of encryption is now routine practice for individuals and businesses. Computer and software manufacturers consider disk encryption a basic security measure and it is a standard feature on most new computers.[1] Device encryption is also a standard feature for the leading smart phone operating systems, Apple IOS and Android.[2] In addition government agencies recommend encryption to protect personal information.[3] In our increasingly connected world where we share and transmit information, encryption is an important an integral part of modern life.

Even though encryption offers presumably millions of people the benefit of safeguarding

---

[1] See Apple, MacOS Security, https://www.apple.com/macos/security; Microsoft, BitLocker, https://docs.microsoft.com/enus/windows/security/information-protection/bitlocker/bitlocker-overview.

[2] See Apple, This is How We Protect Your Security, https://www.apple.com/privacy/approach-to-privacy; Android, Encryption, https://source.android.com/security/encryption/.

[3] See,e.g. 15 USC Section 6801(b) – requiring security measures for consumer financial data / 12 CFR Section 364, App B – interagency rules interpreting Section 6801 to require assessment of need for encryption of that information); 32 CFR Section 310, App. A (E)(1) – requiring encryption for unclassified Department of Defense employee information.

private information, despite the States' contention, encryption is not unbreakable. The States have the ability to use a variety of techniques to gain lawful access to encrypted information without compelling the aid of a criminal suspect. For example, law enforcement could possibly circumvent many forms of encryption by using software or hardware that exploit flaws in the encryption program or the device itself. To illustrate, investigators were able to break the encryption on an IPhone used by the perpetrator of the San Bernardino terrorist attack.[4] Some reports have suggested that law enforcement agencies have contracted with companies and purchased tools to bypass encryption.[5] Further, law enforcement could obtain a warrant to install a camera to record a suspect's key strokes or install software called "keylogger" that captures the characters typed using the device.[6] The above methods, for example, would provide law enforcement with the password without compelling the criminal suspect to provide his or her password.

B. The Court of Appeals' Opinion does not present a technical and legal analysis which renders the government incapable of compelling many suspects to open digital locks.

The States argue that "the Indiana Court of Appeals' Opinion's holding drastically alters the balance of power between investigators and criminals and renders law enforcement often incapable of lawfully accessing relevant information." *Id.* p.11. Encryption does not drastically alter the balance of power. As indicated above, encryption protects important and intimate details of our lives. Technology creates long lasting records of photos, voice recordings, videos, text messages, emails, calendars, internet searches and other various documents and files. Further, our mobile devices create logs of where we have been, who we are with, and where we are going. *See*

[4] FBI unlocks San Bernardino shooter's IPhone and ends legal battle with Apple, for now, LA Times (March 28, 2016)
[5] Joseph Cox, Cops Around the Country Can Now Unlock IPhones, Records Show, Motherboard April 12, 2018, https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police.
[6] Andy Greenerg, Hacker Lexicon: What Is Password Hashing?, Wired (June 8, 2016), Dan Goodin, Why Passwords have never been weaker and crackers never been stronger, Ars Technica (August 20, 2012).

United States v. Jones, 565 US 400, 415 (2012) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations."). Encryption is designed to help to protect the above information in a modern world. As the Eleventh Circuit stated, encryption is not simply a tool for criminals. *Cf. Doe II*, 670 F.3d at 1347 ("Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all.").

In regard to the States' argument that the Court of Appeal's Opinion renders the government incapable of compelling may suspects to open a digital lock, the Opinion itself outlines how to resolve decryption requests from law enforcement authorities. As the Court of Appeals explained:

> 1) "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."
>
> 2) "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."

See K*atelin Eunjoo Seo v. State of Indiana*, 29A05-1710-CR-2466 (Ind. Ct. App.2018).

The States further argue that the Indiana Court of Appeals' Opinion is problematic because

the Opinion states that law enforcement agencies should first attempt to seek the digital data from third parties. The States suggest the most glaring problem is that this would require law enforcement agencies to issues subpoenas. The fact that law enforcement agencies may have to request subpoenas to obtain digital data from third parties is not a compelling argument to circumvent the Fifth Amendment to the Constitution. The States go on to argue that even if issuing a subpoena was possible, not all the information will be available from third parties and some third parties will refuse to comply with subpoenas. If the above is true, as the Indiana Court of Appeals' Opinion provides, law enforcement agencies can still petition the Court indicating their efforts to ***first*** obtain said information from third parties and then identify in a warrant with reasonable particularity the information they seek from the criminal suspect's phone and/or electronic device.

In addition, the States fail to mention that law enforcement agencies do not need ALL information to meet their burden of proof and prosecute a case. For example, the States' proposed drug dealer who keeps records of his drug dealing on a word processor can still be found guilty of dealing. In the States' hypothetical, even if we concede that drug dealers keep an accounting of their drug deals on a word processor, if the criminal suspect possesses a certain amount of drugs he or she can still be prosecuted in Indiana with intent to distribute.[7] In the States' example of a child pornographer who takes pictures with his phone and never sends them over the internet, presumably, law enforcement agencies would have some evidence before they suspected someone of engaging in child pornography. If the criminal suspect is viewing child pornography on an electronic device to take the pictures, then law enforcement agencies could use the IP address to show the criminal suspect viewed certain sites. If the alleged child pornographer is actually taking pictures of live children engaging in pornographic activities, then law enforcement could interview

[7] See IC 35-48-4-10.

third parties, obtain a warrant to search the suspect's home, and utilize a multitude of other tools available to obtain evidence. Upon obtaining that information, the Indiana Court of Appeals' Opinion provides a framework for law enforcement to obtain files from the criminal suspect. In regard to the States' argument that some third parties will refuse to comply with subpoenas, such as Proton Mail, requiring the States to seek assistance from the Swiss government, the States fail to make any mention that law enforcement could require the criminal suspect to sign a release or waiver to obtain said records. In *Doe*, the Court found that a court order compelling the defendant to sign a consent to authorize foreign banks to disclose records of his accounts did not violate his privilege against self-incrimination. *See Doe v. United States*, 487 US 201, 212, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1987).

To further illustrate that the Indiana Court of Appeals' Opinion's does not renders law enforcement incapable of lawfully accessing relevant information, one has to look no further then the case before the Court. After Seo invoked her Fifth Amendment privilege against self-incrimination and refused to unlock the phone at issue, the State of Indiana still pursued criminal prosecution of Seo. Law enforcement was able to obtain evidence from third parties sufficient to resolve not only the case that prompted the search warrant but three (3) additional criminal cases that Seo was being investigated for that dealt with similar issues including the same victim and another partyr, at the time the search warrant for her phone was issued.[8]

C. The Indiana Court of Appeals' Opinion's analysis will preserve the public interest in privacy.

The States argue that if this Court does not reverse the Indiana Court of Appeals' Opinion, the public's interest in solving crimes will cause legislatures to pass draconian anti-privacy laws.

[8] See 29D06-1707-F6-5035; 29D03-1707-CM-5103; 29D03-1709-CM-6974; 29D03-1709-F5-7051

This is mere speculation which presumes the public would view the Court's protection of constitutional rights as a threat against public safety. Moreover, the States are requesting the Court to weigh policy debates like legislatures, rather than to decide questions of law. The States claim that society needs a justice system that does not unduly hamstring law enforcement's efforts to detect and punish wrongdoing. *See* States' Brief p.22. As illustrated above, the Indiana Court of Appeals' Opinion does not "unduly hamstring" law enforcement. In fact, the undersigned counsel believes the true objective of the States' argument is to expand the foregone conclusion doctrine to testimony rather than production of documents, so law enforcement can search the entire contents of a phone and/or electronic device, not only for additional evidence, but also other potential crimes. The States seek the very draconian anti-privacy legislation through the Courts that it advocates against in the States' Brief.

To illustrate this point, Seo has requested the return of her IPhone 7.[9] Seo has no pending criminal cases, has served her executed sentence for the charges relating to the search warrant, and no other search warrants have been requested by law enforcement. Despite these facts, the State of Indiana has objected to Seo's request and seeks to retain her cell phone. The State of Indiana filed a response to Seo's request stating, "Because the reversal of this Court's Contempt Order has been vacated by rule of law, this matter is still pending and all personal property seized pursuant to the Court's search warrant Should remain in the custody of the Hamilton County Sheriff's Department." *See* State's Response to Defendant's Verified Motion to Release Property, filed February 12, 2019, under cause number 29D01-1708—MC-005640. If this Court reverses the Indiana Court of Appeals' Opinion, the State presumably seeks to find Seo in contempt unless she unlocks her IPhone 7. What purpose is there for the State of Indiana to search Seo's phone other

[9] 29D01-1708-MC-5624; 29D01-1708-MC-5640

than to look for other possible crimes?

The States are requesting this Court to apply the foregone conclusion doctrine in such a way that someone under the mere suspicion of a crime that admits ownership of a device can be compelled to unlock the device, such that the State can then search for evidence that it does not even know exists and for potentially additional crimes it has no knowledge ever occurred. The application of the foregone conclusion doctrine to testimony poses significant issues that are explained in more depth below.

IV.

FIFTH AMENDMENT AND THE FOREGONE CONCLUSION DOCTRINE

The States argue that the Indiana Court of Appeals' Opinion "misapprehends the nature of the Fifth Amendment question." See States' Brief p. 14. In regard to the Fifth Amendment, the States appear to draw some distinction between testimony and acts and then acknowledges the Fifth Amendment can apply to an act requiring a criminal suspect to do something.

A. Providing a Password OR Unlocking a Device is Testimonial Communication:

Both the United States Constitution and the State of Indiana Constitution provide protections against self-incrimination. Specifically, the Fifth Amendment of the United States Constitution provides that "No person shall be compelled in any criminal case to be a witness against himself," and Article 1, Section 14 of the Indiana Constitution states "No person in any criminal prosecution shall be compelled to testify against himself." See U.S. Const. Am. 5; IN Const. Art. 1, Sec. 14.

There is no distinction between compelling a criminal suspect to speak his or her password to law enforcement or, by act, enter the password into a phone or computer to unlock the device. The Constitution protects non-verbal acts that communicate the contents of an individual's mind.

Curico v. United States, 354 U.S. 118 (1957). Further, in *Doe v. United States*, 487 US 201, 212, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1987), the Supreme Court found: "An act is testimonial when the accused is forced to reveal his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the government." The Court in *Doe* further stated that "it is the extortion of information from the accused, *the attempt to force him to disclose the contents of his own mind* that implicates the Self-Incrimination Clause." See *id.*, at 211 (emphasis added).

In *United States v. Hubbell*, 530 U.S. 27, 120 (2000), the Supreme Court found that the defendant's assembly of documents in response to a subpoena violated his privilege against self-incrimination. The Court stated: "the assembly of these documents was like telling an inquisitor the combination to a wall safe, not like being forced surrender the key to a strongbox." See *id.*, at 2047. Importantly, the Court in *Hubbell* further stated that: "Compelled testimony that communicates information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory." See *id.*, citing *Doe v. U.*S., 487 U.S. 201, 208, n.6. Further, in *Hoffman v. United States*, 341 US 479, 486 (1951), the Supreme Court emphasized that "the privilege afforded not only extends to answers that would in themselves support a conviction… but likewise furnish a link in the chain of evidence needed to prosecute the claimant…"

Counsel believes the law is well settled that providing a password verbally or by act of production is testimonial and falls under the protection of the Fifth Amendment. Therefore, the analysis moves to whether the foregone conclusion doctrine applies.

The State of Indiana further argues that there is an exception to the act of production doctrine: if doing the act does not give the any additional information, then the result is a foregone conclusion. The States argue that since Seo admitted ownership of the IPhone 7, then it is a foregone conclusion she knows the password. In support of this argument, the State relies on

Fisher v. United States, 425 U.S. 391 (1976), in which the Court found that requiring a client's attorneys to provide documentation prepared by the client's accountants did not violate the client's Fifth Amendment rights against self-incrimination. The Court reasoned: "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." See *id.*, at 421. The foregone conclusion rationale is exceedingly narrow and only relied upon on one occasion to overcome an individual's claim of Fifth Amendment privilege against self-incrimination. See *Fisher*. The foregone conclusion exception applies to only where the States can show with reasonable particularity that it already knows of the materials, thereby making any testimonial aspect a foregone conclusion. See *In Re Grand Jury Subpoena Duces Tecum,* 670 F.3d 1335, 1346 (11th Circuit 2012). There is no foregone conclusion that anything exists on Seo's phone and further in order to apply the foregone conclusion doctrine to Seo's password, the State would have to show that State already knows the password, which the State admittedly does not as it is attempting to compel Seo to unlock her IPhone 7.

Since *Fisher,* the undersigned counsel is unaware of any United States Supreme Court decisions or Federal Court of Appeals decisions where the foregone conclusion doctrine has been applied to testimony. In fact, the foregone conclusion doctrine has overwhelmingly been applied only in cases concerning the compelled production of business and other financial records. Absent guidance from the Supreme Court or the Federal Court of Appeals, this Court should decline the States' request to expand the doctrine's application beyond that narrow scope. If the foregone conclusion where to apply to testimony, then it puts criminal suspects in the cruel predicament of self-accusation, perjury or contempt, which is precisely why the Fifth Amendment exists to save

criminal suspects from self-incrimination. If the Court applies the foregone conclusion to testimony, then criminal suspects could be compelled to testify about potential crimes, if the government could show they already had knowledge of said facts.

If the States were seeking production of documents, then the Eleventh Circuit's decision *In re Grand Jury Subpoena* explains, the appropriate standard, which is similar to the standard articulated by the Indiana Court of Appeals. The Eleventh Circuit began it's analysis by stating a two-part test for determining whether decryption was testimonial:

> 1) Whether the decryption would make use of the contents of his or her mind"; and
>
> 2) Whether the government could show with "reasonable particularity that any testimonial aspects of the decryption were foregone conclusions" because the government "already knew of the materials" sought. *Id* at 1345-46 (citing *Hubbell*, 530 U.S. at 44-45).

That particularity might require knowing "specific file names" or, at a minimum, a showing that government seeks a "certain file" and can establish that "1) the files exist in some specified location, 2) the file is possessed by the target of the subpoena, and 3) the file is authentic." *Id*. at 1349, 28. "Categorical requests for documents the Government anticipates are likely to exist simply will not suffice." *Id* at 1347.

For all the reasons described above, the compelled recollection and use of a memorized password is testimonial and therefore privileged and the foregone conclusion doctrine should not be applied in this case as the States seek to apply the exception to testimony and not the production of documents.

V.

CONCLUSION

WHEREFORE, Appellant, Katelin Eunjoo Seo, respectfully requests that this Court to affirm the Indiana Court of Appeals' Order.

Respectfully Submitted,

__/s/ *William J. Webster*__
William J. Webster, Atty No. 29086-29

VI.

CERTIFICATE OF WORD COUNT

I verify that this brief contains no more than 4,200 words.

/s/ *William J. Webster*
William J. Webster, Atty No. 29086-29

VII.

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was served upon the following on February 28, 2019 by electronic filing using the Court's IEFS system:

Ellen H. Meilaender
Ellen.Meilaender@atg.in.gov

Kenneth J. Faulk
kfalk@aclu-in.org

Kevin S. Smith
ksmith@cchalaw.com

__/s/ *William J. Webster*__
William J. Webster, Atty No. 29086-29
WEBSTER & GARINO LLC
104 N. Union St.
Westfield, IN 46074
Phone: (317) 565-1818
Fax: (317) 758-0100

Attorney for Appellant Katelin Eunjoo Seo