

Brief of Amici Curiae  
State of Utah et al.

IN THE  
INDIANA SUPREME COURT

Case No. 18S-CR-595

KATELIN EUNJOO SEO,	)	Transferred Appeal
	)	from the Indiana Court of Appeals
Appellant,	)	
	)	Court of Appeals case no. 29A05-1710
	)	CR-2466
v.	)	Trial Court Case No. 29D01-1708-MC-
	)	5640
STATE OF INDIANA,	)	Hon. Steven R. Nation
	)	
Appellee.	)	

---

BRIEF OF AMICI CURIAE STATES OF UTAH, GEORGIA, IDAHO, LOUISIANA,  
MONTANA, NEBRASKA, OKLAHOMA, AND PENNSYLVANIA

---

Kevin S. Smith, No. 20379-49  
Special Assistant Utah Attorney General

CHURCH CHURCH HITTLE & ANTRIM  
10765 Lantern Road, Suite 201  
Fishers, IN 46038  
Phone: 317-773-2190  
Email: ksmith@cchalaw.com

*Amicus Counsel* for the States of Utah, Georgia,  
Idaho, Louisiana, Montana, Nebraska,  
Oklahoma, and Pennsylvania

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	3
INTEREST OF AMICI STATES .....	6
ARGUMENT .....	7
Because the lead opinion misunderstands both the nature of decryption and the object of the Fifth Amendment, adopting its reasoning would render States incapable of executing many lawfully obtained warrants. ....	7
A. Modern encryption puts nearly unbreakable locks on digital information. ....	7
B. The lead opinion’s technical and legal analyses render the government incapable of compelling many suspects to open digital locks. ....	11
C. The lead opinion’s analysis could result in less privacy, not more. ....	21
CONCLUSION .....	23
WORD COUNT CERTIFICATE.....	24

## TABLE OF AUTHORITIES

### FEDERAL CASES

<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	21
<i>Doe v. United States</i> , 487 U.S. 201 (1988) .....	14, 15, 17, 20
<i>Fisher v. United States</i> , 425 U.S. 391 (1976).....	15, 17
<i>Hiibel v. Sixth Jud. Dist. Ct. Nev., Humboldt Cty.</i> , 542 U.S. 177 (2004) .....	15
<i>In re Boucher</i> , No. 2:06-mj-91, 2009 WL 424718 (Vt. Dist. Ct. Feb. 19, 2009)...	17
<i>In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011</i> , 670 F.3d 1335 (11th Cir. 2012).....	16
<i>Rios v. United States</i> , 364 U.S. 206 (1960) .....	22
<i>Trainor v. Hernandez</i> , 431 U.S. 434 (1977).....	6
<i>United States v. Apple MacPro Computer</i> , 851 F.3d 238 (3d Cir. 2017) .....	12, 16
<i>United States v. Bright</i> , 596 F.3d 683 (9th Cir. 2010) .....	16
<i>United States v. Fricosu</i> , 841 F.Supp.2d 1232 (D. Colo. 2012).....	17
<i>United States v. Gavegnano</i> , 305 Fed.Appx. 954 (4th Cir. 2009).....	17
<i>United States v. Hubbell</i> , 530 U.S. 27 (2000) .....	18, 22, 23
<i>United States v. Kyles</i> , 40 F.3d 519 (2d Cir. 1994) .....	12
<i>United States v. Spencer</i> , No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018) .....	18, 20

Brief of Amici Curiae  
State of Utah et al.

**STATE CASES**

*Commonwealth v. Baust*, 89 Va. Cir. 267 (2014) ..... 18

*Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. Ct. 2017)..... 17

*Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) ..... 17

*G.A.Q.L. v. State*, 257 So.3d 1058 (Fla. Ct. App. 2018) ..... 16

*Hollars v. State*, 286 N.E.2d 166 (Ind. 1972) ..... 18

*State v. Garcia*, 986 P.2d 491 (N.M. Ct. App. 1999) ..... 13

*State v. Gonzales-Bejarano*, 427 P.3d 251 (Utah Ct. App. 2018) ..... 12

*State v. Mansor*, 421 P.3d 323 (Or. 2018)..... 11

*State v. Stahl*, 206 So.3d 124 (Fla. Dist. Ct. App. 2016) ..... 17

**FEDERAL STATUTES**

U.S. Const. amend. IV ..... 12

U.S. Const. amend. V..... 14

**STATE RULES**

Indiana R. App. P. 44 ..... 24

Brief of Amici Curiae  
State of Utah et al.

**OTHER AUTHORITIES**

25 A.L.R. Fed. 3d Art. 10..... 15

*An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev.  
476 (2011)..... 21

*Encryption Made Simple for Lawyers*, 29 No. 6 GPSolo 18 (2012) ..... 9

*Encryption Workarounds*, 106 Geo. L. J. 989 (2018)..... 7, 8

*Lessons from the British and American Approaches to Compelled Decryption*, 75  
Brook. L. Rev. 345 (2009)..... 22

## INTEREST OF AMICI STATES

Federal and State courts share the “solemn responsibility” to interpret the federal Constitution. *Trainor v. Hernandez*, 431 U.S. 434, 443 (1977) (cleaned up). But because the States shoulder the bulk of the criminal caseload, they do most of the interpretive lifting under the Fourth, Fifth, and Sixth Amendments. Under our common law system, courts facing issues of first impression under the federal constitution invariably look to how courts in sister States have resolved those issues. The persuasive power of those decisions is at its peak when the decision comes from a State court of last resort. Thus, this Court’s decision has the potential to impact not just the law in Indiana, but around the country – particularly where, as here, the issue has divided lower courts. As the top law enforcement officials of their respective jurisdictions, *amici* States Attorneys General have a strong interest in aiding this Court’s decision.

## ARGUMENT

**Because the lead opinion misunderstands both the nature of decryption and the object of the Fifth Amendment, adopting its reasoning would render States incapable of executing many lawfully obtained warrants.**

*Amici* States agree with the State of Indiana that the lead opinion should be reversed. In this brief, *amici* provide additional detail on encryption and the troubling consequences of the lead opinion’s analysis.

### **A. Modern encryption puts nearly unbreakable locks on digital information.**

For as long as people have sent messages, they have devised ways to conceal their meaning from all but the intended recipient. *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 *Geo. L. J.* 989, 993 (2018) (“Cryptology . . . is as old as writing itself.”) (citing David Kahn, *The Codebreakers: The Story of Secret Writing*, 71-106 (1996)); Michael Wachtel, *Give Me Your Password Because Congress Can Say So*, 14 *Pitt. J. Tech. L. & Pol’y* 44, 47 (2013) (discussing Greek and Roman encryption methods). The practice of concealment is called “cryptography,” from the Greek words for

Brief of Amici Curiae  
State of Utah et al.

“secret writing.”<sup>11</sup> To *encrypt* something is to make a message secret; to *decrypt* it is to reveal the secret. *See En-*, Online Etymology Dictionary, <https://www.etymonline.com/word/en-> (last visited Jan. 30, 2019) (en- as prefix means “into” or “in”); *id.* at *De-*, [https://www.etymonline.com/word/de-#etymonline\\_v\\_29283](https://www.etymonline.com/word/de-#etymonline_v_29283) (last visited Jan. 13, 2019) (de- as prefix has “the function of undoing or reversing a verb’s action”). In encryption jargon, the readable message is called the “plaintext,” and the encoded message is “ciphertext.” Kerr & Schneier at 991. But encryption is not limited to text—any digital file or program can be encrypted. *Id.* at 993.

All encryption is based on some algorithm, or series of prescribed steps. *See Algorithm*, Dictionary.com, <https://www.dictionary.com/browse/algorithm> (last visited Jan. 30, 2019). The algorithm may be as simple as substituting one letter for another, as Julius Caesar often did in messages. *See* Wachtel at 47-48. Or it may be as complex as randomly

---

<sup>11</sup> κρυπτός (*kryptos*), meaning “hidden, concealed, secret”; and γραφός (*graphos*), meaning writing. *See Crypto-*, Online Etymology Dictionary, <https://www.etymonline.com/word/crypto-> (last visited Jan. 30, 2019) and *-Graph*, Online Etymology Dictionary, [https://www.etymonline.com/word/-graph#etymonline\\_v\\_48465](https://www.etymonline.com/word/-graph#etymonline_v_48465) (last visited Jan. 30, 2019).

Brief of Amici Curiae  
State of Utah et al.

generating very large numbers to obscure the information. *See* Kerr & Schneier at 993-94 (discussing modern encryption methods). Whatever its form, the algorithm is the metaphorical lock on the data. *See generally* David G. Ries & John W. Simek, *Encryption Made Simple for Lawyers*, 29 No. 6 GPSolo 18 (2012) (Westlaw 2019) (describing encryption types and workings).

Every lock has a key. Like a physical lock, simple algorithms can be picked or broken. In the Caesar example, a few moments' study or a decoder ring would do. *See, e.g., A Christmas Story* (Warner Bros. 1983), [https://youtu.be/zdA\\_\\_2tKoIU](https://youtu.be/zdA__2tKoIU) (last visited Jan. 30, 2019). But the digital keys that safeguard information stored on and transmitted between modern communication devices are made of much sterner stuff. Currently standard digital keys are strings of ones and zeroes ("bits") either 128 or 256 characters long. Kerr & Schneier at 993. A 128-bit key has  $2^{128}$  – or 340,282,366,920,938,463,463,374,607,431,768,211,456 – possible combinations; a 256-bit key, twice that. *Id.* This means that the potential keys for a digital lock could outnumber the grains of sand in the sea and the stars in the universe – combined. *See* Robert Krulwich, *Which is Greater, The Number of*

Brief of Amici Curiae  
State of Utah et al.

*Sand Grains on the Earth or Stars in The Sky?*, NPR (Sept. 17, 2012),  
<https://n.pr/2Rc95pa> (citing sources for estimated 7.5 quintillion  
(7,500,000, 000,000,000,000) sand grains and 70 sextillion (70,000,000,000,000,  
000,000,000) stars).

Thus, in “the arms race between encryption and [decryption], the mathematics overwhelmingly favors encryption.” Kerr & Schneier at 994. 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.* Without the key, the encrypted information remains unreadable.

For the average person, the locks and keys operate automatically or with little input from them – for example, by sending an email or turning off a phone. *See generally* Daniel Garrie & Rick Borden, *Encryption for Lawyers*, ABA Bus. L. Today (Westlaw 2016). Because it’s impractical (to say the least) to memorize 128- or 256-character passcodes and input them every time the user wants access, devices let the user rely on a meta-key, usually in the form of a password (“toomanysecrets”) or biometric data (such as face identification or a fingerprint). *Id.* Entering this information causes the real “key” to decrypt the information. *Id.*

Because they are so much shorter, passwords could be broken using “brute force” methods. To counteract this, companies will limit the number of attempts or the time within which they can be made. If there are enough unsuccessful attempts, the data will be destroyed. *See, e.g.*, Slip op. at 11-12.

**B. The lead opinion’s technical and legal analyses render the government incapable of compelling many suspects to open digital locks.**

The lead opinion’s holding drastically alters the balance of power between investigators and criminals and renders law enforcement often incapable of lawfully accessing relevant evidence.

Most people have smartphones that automatically encrypt their information when not in use. Orin S. Kerr, *Compelled Encryption and the Privilege Against Self-Incrimination*, Tex. L. Rev. (forthcoming 2019) (manuscript at 1 & n.1), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3248286](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248286) (last visited Jan. 30, 2019) (citing source stating that “94% of those aged 18-29 own a smartphone,” “many of which encrypt their data by default when not in use”). Other digital storage devices – such as laptops, tablet computers, and thumb drives – are easily encryptable and often encrypted, sometimes in very sophisticated ways. *Id.*; *see also State v. Mansor*,

Brief of Amici Curiae  
State of Utah et al.

421 P.3d 323, 331-33 (Or. 2018) (discussing other methods of hiding digital information).

As everyone knows, these devices hold vast amounts of our information. For criminals, this often includes information on their crimes – files of child pornography, or texts and ledgers of drug dealing, for example. *See, e.g., United States v. Apple MacPro Computer*, 851 F.3d 238, 247-48 (3d Cir. 2017) (encrypted child pornography on external hard drives); *State v. Gonzales-Bejarano*, 427 P.3d 251, 253-54 & n.1 (Utah Ct. App. 2018) (drug dealer discussing using encrypted smartphone application to set up drug deals). This means that many cases are built in part on digital evidence of one kind or another. Indeed, it is increasingly rare to have a case that does *not* include digital evidence.

Absent consent to search or a very rare exigency, the government must get a warrant, showing a magistrate that there is probable cause to access this locked information. U.S. Const. amend. IV. In any other context – a strongbox, a storage container, a home – that warrant authorizes police to open the container by force if necessary and obtain the evidence. *See, e.g., United States v. Kyles*, 40 F.3d 519, 522-23 (2d Cir. 1994) (affirming

Brief of Amici Curiae  
State of Utah et al.

admission of evidence where police broke lock on door inside home); *State v. Garcia*, 986 P.2d 491, 494 (N.M. Ct. App. 1999) (citing cases involving removing screws and carpeting, puncturing metal containers, breaking lock on trunk of car); *see also Semayne's Case*, 5 Co. Rep. 91a, 91a, 77 Eng. Rep. 194, 194 (K.B. 1603) (“In all cases where the King is party, the sheriff may break the house, either to arrest or do other execution of the King’s process, if he cannot otherwise enter.”). Where the criminal has an essentially unbreakable digital lock, “brute force” methods are not available. The government must be able to compel the suspect to use the key and open the lock. But under the lead opinion’s analysis, compelling the lock open is impossible in many cases.

The lead opinion’s reasoning is incorrect in three respects: First, it misapprehends how encryption works; second, it misapprehends the object of the Fifth Amendment question; and third, it creates – as the dissent explains – a “zone of lawlessness” for criminals to operate in.

The lead opinion misunderstands the nature of encryption. In its view, every time information is encrypted and decrypted, it is essentially destroyed and created anew. *See Slip op.* at 30. But that is not correct. As

Brief of Amici Curiae  
State of Utah et al.

explained above, entering a passcode does not “re-create” the content; it merely renders it readable. Making encrypted information readable does not “re-create” its content any more than putting on a pair of reading glasses “re-creates” the contents of the morning newspaper. In either case, the content never changes – only the user’s ability to access it does.

The lead opinion also misapprehends the nature of the Fifth Amendment question. The Fifth Amendment protects a person from being “compelled in any criminal case to be a witness against himself.” U.S. Const. amend. V. In the prototypical case, this prevents the government from using coercion to force people to admit their guilt. *See generally Doe v. United States*, 487 U.S. 201, 210-12 (1988) (discussing history of the clause and Star Chamber practices). But it can also apply to coercing incriminating information.

“The basic idea is that complying with an order to *do* something can send a message just like complying with an order to *say* something.” Kerr, *Compelled Decryption* at 6. Such “acts of production” violate the Fifth Amendment if the action is: (1) compelled; (2) testimonial (in that it requires the person to reveal the contents of their mind); and (3) incriminating. *Id.* at

Brief of Amici Curiae  
State of Utah et al.

5-6 (citing *Hiibel v. Sixth Jud. Dist. Ct. Nev., Humboldt Cty.*, 542 U.S. 177, 189-90 (2004); *Doe*, 487 U.S. at 210-11; *Fisher v. United States*, 425 U.S. 391, 410 (1976)); see also 25 A.L.R. Fed. 3d Art. 10, *Construction and Application of "Foregone Conclusion" Exception to the Fifth Amendment Privilege Against Self-Incrimination*, § 2 (Westlaw 2019) (citing cases applying doctrine to electronic records and devices).

There is an exception to the act-of-production doctrine: if doing the act does not give the government any additional information, then the result is a "foregone conclusion." *Fisher*, 425 U.S. at 411. To meet the foregone-conclusion exception, the government must show (1) knowledge of the information demanded; (2) the defendant's possession of it; and (3) its authenticity. *Fisher*, 425 U.S. 410-13; see also *Doe*, 465 U.S. at 613-14 & n.11-13.

The lead opinion acknowledges the foregone conclusion exception, Slip op. at 26-36, but misapplies it. In the lead opinion's view, the "information demanded" is the content of the container, not opening the lock. *Id.* In other words, to get to the contents, the State must first identify those contents. *Id.* Other courts have labored under this same misconception, which imposes an impossible burden in many cases. See,

Brief of Amici Curiae  
State of Utah et al.

*e.g.*, *Apple MacPro Computer*, 851 F.3d at 247 (applying foregone conclusion doctrine to contents, not password); *United States v. Bright*, 596 F.3d 683, 692 (9th Cir. 2010) (similar); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (similar); *G.A.Q.L. v. State*, 257 So.3d 1058, 1063 (Fla. Ct. App. 2018) (“It is critical to note here that when it comes to data locked behind a passcode wall, the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall.”).

Contrary to these decisions, entering a password communicates only a single thing: that the person knows the password. *Kerr, Compelled Disclosure* at 16-17. It is the forced opening of the lock – not the contents – that meets the act-of-production test: the act is compelled, it is testimonial (comes from the mind), and it is incriminating (shows the person owns or at least has access). And where (as here) the unlocking provides the government with no additional information, then the unlocking supports a mere foregone conclusion, and the government can compel it.

While it is true that opening the lock provides access to the contents, the contents were not forced from the defendant’s mind. Because the

Brief of Amici Curiae  
State of Utah et al.

contents are neither compelled nor testimonial, the Fifth Amendment applies only to the unlocking, not to the contents. *See id.* at 3, 12-13, 16, 21 (distinguishing act of “door-opening” from the non-testimonial “treasure” inside); *see also Fisher*, 425 U.S. at 409-10 (underlying documents not privileged); *Doe*, 465 U.S. at 611-12 (“Although the contents of a document may not be privileged, the act of producing the document may be.”); *United States v. Gavegnano*, 305 Fed.Appx. 954, 956 (4th Cir. 2009) (applying foregone conclusion doctrine to password, not contents); *United States v. Fricosu*, 841 F.Supp.2d 1232, 1236 (D. Colo. 2012) (similar); *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718, at \*2 (Vt. Dist. Ct. Feb. 19, 2009) (“There is no question that the contents of the laptop were voluntarily prepared or compiled and are not testimonial, and therefore do not enjoy Fifth Amendment protection.”); *State v. Stahl*, 206 So.3d 124, 136 (Fla. Dist. Ct. App. 2016) (applying foregone conclusion doctrine to password); *Commonwealth v. Gelfatt*, 11 N.E.3d 605, 615 (Mass. 2014) (holding that act of entering encryption keys in computers were foregone conclusions and that “the act of decryption is not a testimonial communication that is protected by the Fifth Amendment”); *Commonwealth v. Davis*, 176 A.3d 869,

Brief of Amici Curiae  
State of Utah et al.

875-76 (Pa. Super. Ct. 2017) (applying foregone conclusion doctrine to password, not contents); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (2014) (holding Fifth Amendment applicable to password, but not contents of smartphone). By applying the foregone conclusion doctrine to the contents rather than the unlocking, the lead opinion misconstrues the Fifth Amendment.<sup>2</sup>

---

<sup>2</sup> The lead opinion also equates passwords with biometric data. *See* Slip op. at 13 n.11. But the Fifth Amendment does not apply to biometric data – fingerprints, faces, and the like – because nothing is being compelled from the defendant’s mind. *See Hollars v. State*, 286 N.E.2d 166, 168 (Ind. 1972) (holding that Fifth Amendment privilege against self- incrimination “does not shield against compulsory submission to tests that are merely physical or produce evidence that is only physical in nature, such as fingerprints, measurements, voice or handwriting exemplars, or physical characteristics or abilities”). In this respect, biometrics are akin to a suspect being forced to put on a shirt, or to give a blood sample, a handwriting exemplar, or a voice recording. *See United States v. Hubbell*, 530 U.S. 27, 35 (2000) (“[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.”). This further shows the breadth of the lead opinion’s sweep.

But even setting the biometrics/password distinction aside, constitutionally favoring one form of encryption over another will merely drive more criminals to adopt that form. *See United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at \*2 (N.D. Cal. Apr. 26, 2018) (reasoning that it would make no sense for Fifth Amendment analysis to turn on form of encryption). Whatever the key, the analysis should focus on the act of unlocking, not the contents.

Brief of Amici Curiae  
State of Utah et al.

The lead opinion's misconceptions carry serious consequences: "suspects could take simple steps to introduce testimonial doors that block access to their non-testimonial treasures." Kerr, *Compelled Decryption* at 12-13. Any time a suspect password-protected a device or a file, it would be impossible to force him to unlock it – even if the government had secured a valid warrant. The Fifth Amendment should not be forged into a sword against the Fourth. This would create the "zone[s] of lawlessness" that Judge May warned of. Slip op. at 50.

The lead opinion tries to limit its broad holding by saying that the State could simply access the same data from third-party providers. Slip op. at 43. But there are problems with this approach. Most glaringly, it would require the State to take an additional step of issuing subpoenas when it has already secured a valid warrant. But even if subpoenas could issue, not all of the information will be available from third parties for two reasons. First, content can be created and stored on electronic devices without sending it through a third party. For example, a drug dealer could keep a ledger of sales using a word processor and never send it through email or cloud storage. Or a child pornographer may take pictures with his phone that he

Brief of Amici Curiae  
State of Utah et al.

stores on the phone itself, or an external hard drive, and never send them over the internet. Sending a subpoena to a third party (like Google or Facebook) will produce none of this relevant evidence.

Second, some third parties will refuse to comply with subpoenas. Consider a free-for-download encrypted email service, ProtonMail. ProtonMail touts itself as a “secure” service “based in Switzerland” subject to “strict Swiss privacy laws.” See ProtonMail, <https://protonmail.com/> (last visited Jan. 30, 2019). It purports to render email “completely invisible.” *Id.* ProtonMail refuses to turn over any user information unless it receives notice from the Geneva Public Prosecutor’s office or the Swiss Federal Police that there is a valid warrant issued from a Canton court or Swiss Federal Supreme Court. See *Privacy Policy*, ProtonMail, <https://protonmail.com/privacy-policy> (last visited Jan. 30, 2019). States are unlikely to convince a foreign government to issue subpoenas in aid of a local investigation. *Cf. Doe*, 487 U.S. at 203 n.1 (noting difficulty of obtaining bank records from foreign government without account owner’s permission).

**C. The lead opinion’s analysis could result in less privacy, not more.**

The lead opinion touts the need for greater privacy protections in an era when ever-increasing portions of our lives are digitized and stored electronically. Slip op. at 36-43. This concern is understandable, but misplaced. Privacy is the domain of the Fourth Amendment, not the Fifth Amendment. *See Kerr, Compelled Decryption* at 29-30, 35. And the Supreme Court has already begun to address the lead opinion’s concern in the Fourth Amendment context. *See Carpenter v. United States*, 138 S. Ct. 2206, 2219-21 (2018) (noting pervasiveness of cell phones and requiring government to “get a warrant” for cell phone location information).

Even if the same sort of policy concerns did inform the Fifth Amendment inquiry, the balance would still favor compelled disclosure. Fourth Amendment jurisprudence is largely a balancing of private and governmental interests. *Kerr, Compelled Decryption* at 28; Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011). If the Fifth Amendment analysis included such balancing questions, the proper view would show that decryption has shifted the balance of power away from government and towards privacy. *Kerr, Compelled*

Brief of Amici Curiae  
State of Utah et al.

*Decryption* at 30-35. In many ways, “the widespread use of strong encryption by users” – and investigators’ corresponding inability to access it without compulsion – has created a “reverse-Carpenter” situation: “Instead of technology expanding government power in ways that call for new rules to avoid Big Brother, widespread encryption limits government power to execute otherwise lawful searches.” *Id.* at 34; *see also* Brendan M.

Palfreyman, *Lessons from the British and American Approaches to Compelled Decryption*, 75 *Brook. L. Rev.* 345, 347 (2009) (“The consequences of the ubiquitous use of unbreakable encryption by criminals like terrorists, hackers, child pornographers, and members of organized crime syndicates, to name a few, would be devastating.”).

Society needs a justice system that does not unduly hamstring law enforcement’s efforts to detect and punish wrongdoing. “The pertinent general principle, responding to the deepest needs of society, is that society is entitled to every man’s evidence.” *Rios v. United States*, 364 U.S. 206, 234 (1960) (Frankfurter, J., dissenting). In a sense, “the public interest in solving crime is something like the force of a river. Technology can influence it, but the water will get downhill somehow.” Kerr, *Compelled Disclosure* at 36-37. If

criminals could easily defeat any warrant simply by “going dark” through encryption, then “the public’s interest in solving crimes will encourage other alternatives,” such as draconian anti-privacy legislation. *Id.* at 37; *see, e.g.,* Palfreyman at 346-47. (discussing “decidedly pro-law enforcement” legislation in the United Kingdom to compel decryption). Ironically, the lead opinion’s rule could tend to undermine the very privacy that it purportedly sought to protect.

Finally, to the extent that the court is concerned that the compelled act of opening a lock will be used against the defendant, it could impose an exclusionary rule on that communicative act. Kerr, *Compelled Decryption* at 10-11. The government would be able to access the files, but would not be able to use the unlocking itself as evidence against him.

## CONCLUSION

The lead opinion misunderstands what encryption does and what communicative acts the Fifth Amendment applies to. These misunderstandings lead to an opinion that, if adopted, renders the government incapable of executing lawfully obtained warrants in many cases. Ironically, it also undermines the very privacy rights it purports to

Brief of Amici Curiae  
State of Utah et al.

protect. To be sure, digital privacy is an ever-growing concern. But that concern does not justify fashioning the Fifth Amendment into a sword against the Fourth Amendment and the public need for relevant evidence. This Court should reverse.

Respectfully submitted,

/s/ Kevin S. Smith

Kevin S. Smith, No. 20379-49  
Special Assistant Utah Attorney General

CHURCH CHURCH HITTLE & ANTRIM  
10765 Lantern Road, Suite 201  
Fishers, IN 46038  
Phone: 317-773-2190  
Email: ksmith@cchalaw.com

*Amicus Counsel* for the States of Utah,  
Georgia, Idaho, Louisiana, Montana,  
Nebraska, Oklahoma, and Pennsylvania

### **WORD COUNT CERTIFICATE**

I verify that in compliance with rule 44(E) and (F), Indiana Rules of Appellate Procedure, this brief contains less than 4,200 words, excluding the table of contents, table of authorities, and certificates of counsel.

/s/ Kevin S. Smith

Kevin S. Smith, No. 20379-49

Brief of Amici Curiae  
State of Utah et al.

### CERTIFICATE OF SERVICE

Undersigned counsel certifies that, on January 31, 2019, the foregoing was electronically filed using the Court's IEFS system and service was made on the following through E-service using the IEFS:

William J. Webster  
wwebster@websterlegal.com  
Carla V. Garino  
cgarino@websterlegal.com

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

*/s/ Kevin S. Smith*

\_\_\_\_\_  
Kevin S. Smith, No. 20379-49