No. 19-1254

In the Supreme Court of the United States

COMMONWEALTH OF PENNSYLVANIA,
Petitioner,

v.

JOSEPH J. DAVIS,
Respondent.

On Petition for Writ of Certiorari to the Pennsylvania Supreme Court

BRIEF OF *AMICI CURIAE* STATES OF UTAH, ALABAMA, ARKANSAS, CONNECTICUT, FLORIDA, GEORGIA, IDAHO, INDIANA, IOWA, KANSAS, LOUISIANA, MARYLAND, MONTANA, NEBRASKA, NEW JERSEY, NEW MEXICO, NORTH DAKOTA, OHIO, OKLAHOMA, SOUTH CAROLINA, SOUTH DAKOTA, AND TEXAS SUPPORTING PETITIONER

SEAN D. REYES
Utah Attorney General
TYLER R. GREEN*
Utah Solicitor General
THOMAS B. BRUNKER
Deputy Solicitor General
JOHN J. NIELSEN
Assistant Solicitor General
350 N. State Street, Suite 230
Salt Lake City, UT 84114-2320
(801) 538-9600
tylergreen@agutah.gov
**Counsel of Record*

Counsel for Amicus Curiae State of Utah

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

May courts require a suspect to unlock an electronic device subject to a search warrant—or hold them in contempt for refusing to do so? Lower courts have split on this important question. And given the ubiquity of those devices, they are an increasingly important source of evidence in criminal cases. As the top law enforcement officials of their respective jurisdictions, *amici* State Attorneys General have a strong interest in getting clarity on the important Fifth Amendment question here. Its answer could affect almost every criminal case.

INTRODUCTION AND SUMMARY OF ARGUMENT

Personal electronic devices—cell phones, computers, and data storage devices—are everywhere. Nearly everyone uses them nearly every day. Criminals are no different. They use them to commit just about every crime imaginable, from scheduling drug deals and setting up murders to creating and storing child pornography. This sort of evidence is increasingly important to law enforcement and is often sought through a warrant.

Amici States agree with Pennsylvania that this Court should grant review and reverse the Pennsylvania Supreme Court. In this brief, *amici* provide additional detail on encryption and the troubling consequences of the lower court's analysis.

---

[1] *Amici* timely notified counsel for all parties of their intention to file this brief.

ARGUMENT

I. This Court should grant review to prevent suspects from misusing the Fifth Amendment to block execution of valid warrants.

The Pennsylvania Supreme Court's holding and others like it effectively prevent law enforcement from unlocking an electronic device—even with a warrant—if a defendant objects. In this brief, *amici* provide additional detail on encryption and the troubling consequences of the court's analysis below.

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) (Kerr & Schneier) ("Cryptology . . . is as old as writing itself.") (citation omitted); Michael Wachtel, *Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals Regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind*, 14 Pitt. J. Tech. L. & Pol'y 44, 47-48 (2013) (Wachtel) (discussing Greek and Roman encryption methods). The practice of concealment is called "cryptography," from the Greek words for "secret writing."[2] To *en*crypt something is to

[2] κρυπτός (kryptos), meaning "hidden, concealed, secret"; and γραφός (graphos), meaning writing. *See Crypto-*, Online Etymology Dictionary, https://www.etymonline.com/word/ crypto- and *-Graph*, Online Etymology Dictionary, https://www.etymonline.com/word/-graph.

make a message secret; to *de*crypt it is to reveal the secret. *See En-*, Online Etymology Dictionary, https://www.etymonline.com/word/en- (en- as prefix means "into" or "in"); *id.* at *De-*, https://www.etymonline .com/word/de- (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 990-91. 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. 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 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. 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, exponentially more. *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 Sand Grains on Earth or Stars in The Sky*?, Krulwich Wonders: Robert Krulwich on Science, 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*, 2016-JUN Bus. L. Today 1, 1-3 (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). Kerr & Schneier at 994. 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 might be destroyed. *See, e.g.*, *Seo v. State*, 109 N.E.3d 418, 425 (Ind. Ct. App. 2018), *vacated and review granted by* 119 N.E.3d 90 (Ind. 2018).

B. The legal analysis below renders law enforcement incapable of executing warrants to access evidence hidden behind most digital locks.

The Pennsylvania Supreme Court held that requiring a suspect to unlock a device using a password would violate the Fifth Amendment because it would force information from his mind. Pet. App. 22a-24a. Adopting this analysis would drastically alter the balance of power between investigators and criminals and often render law enforcement incapable of lawfully accessing relevant evidence.

Most people have smartphones that automatically encrypt their information when not in use. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 768 n.1 (2019) (Kerr) (explaining that 94% of 18- to 29-year-olds 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.* at 768 & n.2; *see also State v. Mansor*, 421 P.3d 323, 331-33 (Or. 2018) (discussing 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 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, criminal cases without digital evidence are increasingly rare.

Absent consent to search or a very rare exigency, law enforcement must get a warrant, showing a neutral and detached 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. That has been the rule for more than 400 years. *See, e.g., United States v. Kyles*, 40 F.3d 519, 522-23 (2d Cir. 1994) (affirming 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, 91b, 77 Eng. Rep. 194, 195 (K.B. 1603) ("[W]hen the King is party, the sheriff (if the doors be not open) may break the party's house, either to arrest him, or do other execution of the King's process, if otherwise he cannot enter.").

But when the suspect has an essentially unbreakable digital lock, brute force methods are either not available at all or very expensive.[3] Courts must be able to compel the suspect to use the key and open the lock—or punish him for refusing.

Yet under the lower court's analysis, compelling the lock open is impossible in many cases. The lower court went wrong because it misapprehended the nature of the right against self-incrimination.

---

[3] Some companies claim that they are able to defeat any and all encryption forms. *See, e.g.,* Cellebrite, https://www.cellebrite.com/en/law-enforcement/lab/ (claiming to be able to help law enforcement "[c]rack into evidence from the widest range of devices, even those at the leading edge of the market, with advanced techniques," and that "[u]ser lock and encryption barriers are no match for Cellebrite UFED technology and services."). But these services are expensive. *See* SC Media, *Cellebrite UFED Series*, https://www.scmagazine.com/review/cellebrite-ufed-series/ (stating that UFED device "starts at $9,000" and can cost as much as $15,999). And in the very recent past, that encryption was unbreakable.. *See, e.g., State v. Johnson*, 576 S.W.3d 205, 218 n.4 (Mo. Ct. App. 2019) (explaining that Cellebrite technology at the time unable to bypass encryption on iPhone). Routinely requiring police to break digital locks would be financially untenable, even if technically possible in a given case. And what is possible today may be impossible tomorrow, since "the mathematics overwhelmingly favors encryption" in the digital arms race. Kerr & Schneier at 994.

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 forcing someone to admit 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 actions.

"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 at 772. 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 771 (citing *Hiibel v. Sixth Jud. Dist. Ct.*, 542 U.S. 177, 189 (2004); *Doe*, 487 U.S. at 210-11, 215; *Fisher v. United States*, 425 U.S. 391, 410 (1976)); *see also* Fern L. Kletter, *Construction and Application of "Foregone Conclusion" Exception to Fifth Amendment Privilege Against Self-Incrimination*, 25 A.L.R. Fed. 3d Art. 10, § 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. *Id.* at 410-13; *see also United States v. Doe*, 465 U.S. 605, 613-14 & n.11-13 (1984).

The lower court acknowledged this exception, but misapplied it. Pet. App. 26a-30a. In its view, the "information demanded" was the content of the container, not opening the lock. *Id.* at 30a-31a; *see also Seo*, 109 N.E.3d at 432-36. In other words, to get to the contents, the State must first identify those contents. Other courts have labored under this same misconception, which imposes an impossible burden in many cases. *See, 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, 692-94 (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 at 769-70. 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 it meets the foregone conclusion exception, 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 contents are neither compelled nor testimonial, the Fifth Amendment applies only to the unlocking, not to the contents. *See id.* at 771, 776-78 (distinguishing act of "door-opening" from the non-testimonial "treasure" inside); *see also Fisher*, 425 U.S. at 409-10 & n.11 (holding 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); *Matter of the Search of a Residence in Aptos, California 95003*, 2018 WL 1400401, *6 (N.D. Cal., Mar. 20, 2018) (same); *United States v. Fricosu*, 841 F.Supp.2d 1232, 1236-37 (D. Colo. 2012) (similar); *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718, at *2 (D. Vt., Feb. 19, 2009); *State v. Stahl*, 206 So.3d 124, 136 (Fla. Dist. Ct. App. 2016) (applying foregone conclusion doctrine to password); *Commonwealth v. Gelfgatt*, 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"); *State v. Johnson*, 576 S.W.3d 205, 227 (Mo. Ct. App. 2019) (similar); *State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. Ct. App. Div. 2018) (similar); *State v. Pittman*, 452 P.3d 1011, 1014, 1022 (Or. Ct. App. 2019) (similar, reaching same result under both Fifth Amendment and state constitution); ("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."); *Commonwealth v. Davis*, 176

A.3d 869, 875-76 (Pa. Super. Ct. 2017) (applying foregone conclusion doctrine to password, not contents), *overruled by Pennsylvania v. Davis*, 220 A.3d 534 (Pa. 2020); *Commonwealth v. Baust*, 89 Va. Cir. 267, *4 (2014) (holding Fifth Amendment applicable to password, but not contents of smartphone); *cf. United States v. Robinson*, 76 M.J. 663, 671 (A.F. Crim. App. 2017) (holding that police requesting password was not interrogation under *Miranda* because password knowledge was foregone conclusion).

By applying the foregone conclusion doctrine to the contents rather than the unlocking, cases like the one below misconstrue the Fifth Amendment.[4] This

[4] One court has also equated passwords with biometric data. *See Seo*, 109 N.E.3d at 425 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 State v. Diamond*, 905 N.W.2d 870, 872 (Minn. 2018) (holding Fifth Amendment does not apply to compelled fingerprint unlocking of cell phone); *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.").

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.

misconception carries serious consequences: "suspects could take simple steps to introduce testimonial doors that block access to their non-testimonial treasure." Kerr at 777. Any time a suspect password-protected a device or a file, it would be impossible to force him to unlock it—even if law enforcement had secured a valid warrant. This would create "zone[s] of lawlessness" that the police could not police. *Seo*, 109 N.E.3d at 443 (citation omitted) (May, J., dissenting).

Some courts try to limit their broad holdings by saying that the State could simply access the same data from third-party providers. *See, e.g., Seo*, 109 N.E.3d at 439. But there are problems with this approach. Most glaringly, it would require the State to take the additional step of issuing subpoenas when it has already secured a valid warrant. And 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 and store them on the phone itself, or on 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.

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.

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/. 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 "competent Swiss authorities," such as a Canton court or Swiss Federal Supreme Court. *See Privacy Policy*, ProtonMail, https://protonmail.com/privacy-policy. 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 lower court's analysis could result in less privacy, not more.

Many opinions on the Pennsylvania side of the split tout the need for greater privacy protections in an era when ever-increasing portions of our lives are digitized and stored electronically. *See, e.g., Seo*, 109 N.E.3d at 420. This concern is understandable, but misplaced in the context of these types of cases. Privacy is the domain of the Fourth Amendment, not the Fifth Amendment. *See* Kerr at 787. And this Court has already begun to address that 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 at 791; 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 encryption has shifted the balance of power away from law enforcement and towards privacy. Kerr at 770. 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 796; *see also* Brendan M. Palfreyman, *Lessons from the British and American Approaches to Compelled Decryption*, 75 Brook. L. Rev. 345, 347 (2009) (Palfreyman) ("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. 233, 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 at 798. 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.*; *see, e.g.,* Palfreyman, 75 Brook. L. Rev. at 346-47. (discussing "decidedly pro-law enforcement" legislation in the United Kingdom to compel decryption). Ironically, the opinion below could tend to undermine the very privacy that it purportedly sought to protect.

CONCLUSION

The Pennyslvania Supreme Court and others adopting like reasoning misunderstand what communicative acts the Fifth Amendment applies to. This misunderstanding leads to a theory that, if adopted, renders law enforcement incapable of executing lawfully obtained warrants in many cases. Ironically, it also undermines the very privacy rights it purports to protect. To be sure, digital privacy is an ever-growing concern. But the Fourth Amendment – not the Fifth – protects privacy. And the right against self-incrimination should not become a get-out-of-investigation-free card, blocking valid warrant execution and preventing discovery of relevant, non-testimonial evidence. This Court should grant review and reverse.

Respectfully submitted.

SEAN D. REYES
Utah Attorney General
TYLER R. GREEN*
Utah Solicitor General
THOMAS B. BRUNKER
Deputy Solicitor General
JOHN J. NIELSEN
Assistant Solicitor General
350 N. State Street, Suite 230
Salt Lake City, UT 84114-2320
(801) 538-9600
tylergreen@agutah.gov

**Counsel of Record*

Counsel for State of Utah

ADDITIONAL COUNSEL

STEVE MARSHALL
Attorney General
STATE OF ALABAMA

TOM MILLER
Attorney General
STATE OF IOWA

LESLIE RUTLEDGE
Attorney General
STATE OF ARKANSAS

DEREK SCHMIDT
Attorney General
STATE OF KANSAS

RICHARD J. COANGELO, JR.
Chief State's Attorney
STATE OF CONNECTICUT

JEFF LANDRY
Attorney General
STATE OF LOUISIANA

ASHLEY MOODY
Attorney General
STATE OF FLORIDA

BRIAN E. FROSH
Attorney General
STATE OF MARYLAND

CHRISTOPHER M. CARR
Attorney General
STATE OF GEORGIA

TIMOTHY C. FOX
Attorney General
STATE OF MONTANA

LAWRENCE WASDEN
Attorney General
STATE OF IDAHO

DOUG PETERSON
Attorney General
STATE OF NEBRASKA

AARON NEGANGARD
Chief Deputy
Attorney General
STATE OF INDIANA

GURBIR S. GREWAL
Attorney General
STATE OF NEW JERSEY

HECTOR H. BALDERAS
Attorney General
STATE OF NEW MEXICO

WAYNE STENEHJEM
Attorney General
STATE OF NORTH DAKOTA

DAVID YOST
Attorney General
STATE OF OHIO

MIKE HUNTER
Attorney General
STATE OF OKLAHOMA

ALAN WILSON
Attorney General
STATE OF SOUTH CAROLINA

JASON R. RAVNSBORG
Attorney General
STATE OF SOUTH DAKOTA

KEN PAXTON
Attorney General
STATE OF TEXAS