1-1-2019

What Am I Really Saying When I Open My Smartphone: A Response to Prof. Kerr

Laurent Sacharoff
University of Denver, lsacharoff@law.du.edu

What Am I Really Saying When I Open My Smartphone: A Response to Prof. Kerr

Publication Statement

Copyright held by the author. User is responsible for all copyright compliance.

Originally published as Laurent Sacharoff, What Am I Really Saying When I Open My Smartphone: A Response to Prof. Kerr, 97 Tex. L. Rev. Online 63 (2019).

Texas Law Review Online
Volume 97

Response

What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr

Laurent Sacharoff*

In his article, *Compelled Decryption and the Privilege Against Self-Incrimination*,[1] Orin S. Kerr addresses a common question confronting courts: if a court orders a suspect or defendant to enter her password to open a smartphone or other device as part of a law-enforcement investigation, does that order violate the Fifth Amendment right against self-incrimination? The question turns out to be surprisingly tricky. It requires us to untangle the existing Fifth Amendment case law as applied to document subpoenas, the "act of production" doctrine, and its mysterious cousin, the "foregone conclusion" doctrine.

From this tangle, Kerr helpfully proposes a simple rule: if the government can independently show the person knows the password to the device, it may compel her to enter her password to open it. Kerr gleans this rule by analogy to a person responding to a document subpoena; under Supreme Court precedent, that person has a Fifth Amendment right against producing documents if the very act of producing them would itself be testimonial and incriminating.

But when we consider the analogy to the act-of-production cases closely, and match like to like, we really should arrive at a rule different from Kerr's. The rule should not be, as Kerr argues, whether the government can

*Professor of Law, University of Arkansas School of Law, Fayetteville; J.D., Columbia Law School; B.A., Princeton University. The author has also previously published with the *Texas Law Review*. Laurent Sacharoff, *Former Presidents and Executive Privilege*, 88 TEXAS L. REV. 301 (2009).

1. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEXAS L. REV. 767 (2019).

show the suspect knows the password to the device.[2] Rather, the rule should be whether the government already knows the person possesses the files on the device and can identify them with reasonable particularity.[3] This rule, after all, is precisely what the case law requires in an ordinary document-production situation.[4]

Which of these two rules should govern depends, roughly speaking, upon whether this foregone conclusion doctrine applies to the password only or to the files on the device as well. This debate has divided courts recently.[5] In fact, some courts holding[6] that the government must merely establish that the suspect knows the password have often cited Kerr's argument made earlier in blog posts that have ultimately led to his more serious consideration here.

The difficulty arises because the act of production doctrine itself, and therefore the foregone conclusion doctrine, rest upon a faulty premise. Courts and some scholars including Kerr rarely discuss this flaw and how it infects the entire act-of-production enterprise. This short response piece shows how we must address this flaw before applying the act of production doctrine to the new situation of passwords.

Below, I first sketch the act of production doctrine as it applies to ordinary document productions, along with its faulty premise, before applying the analogy to entering passwords to unlock devices. I then try to show why Kerr's simple rule does not follow from the existing case law, in part because he has failed to take account of this faulty premise. Finally, I assess Kerr's larger normative argument.

I. The Act of Production and Its Faulty Premise

We must first clear away what question we are not addressing. We are not addressing whether the government can compel a suspect to orally state, or write down, her passcode. Such compulsion would violate the Fifth Amendment,[7] as almost everyone including Kerr[8] agrees.[9]

---

2. *Id.* at 782–83.

3. Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 208 (2018).

4. Fisher v. United States, 425 U.S. 391, 411 (1976); United States v. Greenfield, 831 F.3d 106, 116 (2d Cir. 2016).

5. *Compare In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012) (foregone conclusion doctrine applies to documents sought), *and In re* the Search of a Residence in Oakland, California, No. 4-19-70053, 2019 WL 176937, at *4 (N.D. Cal. Jan. 10, 2019) (same), *with* United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (it applies to the password only); *see also* United States v. Apple MacPro Computer, 851 F.3d 238, 248 & n.7 (3d Cir. 2017), *cert. denied*, 138 S. Ct. 1988 (2018) (mem.) (stating in dicta that the doctrine applies to knowledge of password only).

6. *E.g.*, *Spencer*, 2018 WL 1964588, at *3 & n.2.

7. Sacharoff, *supra* note 3, at 223.

8. *See* Kerr, *supra* note 1, at 778–79.

9. *Spencer*, 2018 WL 1964588, at *2 ("For instance, the government could not compel Spencer to state the password itself, whether orally or in writing.").

Instead, we address a far stranger situation: the government compels a person to enter her password in such a manner that no one else sees or records the password, and the device itself makes no permanent record of it. Entering the password merely opens the device. Does this *act* enjoy Fifth Amendment protection?

Now we could simply say "no," and call it a day. That is, we could say that this act of opening a device enjoys no Fifth Amendment protection at all because it is a pure physical act, no different from giving blood for a blood alcohol test—an act unprotected by the Fifth Amendment.[10] But neither Kerr nor the courts have taken this route. Rather, they have decided that opening a device to reveal to the police all the documents, files, and images it contains counts as more than a pure physical act. It enjoys enough similarities to a document production that the act enjoys some Fifth Amendment protection in some circumstances.

A. The Doctrine

The Fifth Amendment does not protect the contents of papers that a suspect may have previously created. As the Court held in *Fisher v. United States*,[11] the government did not compel the person to create the writing, and in compelling their production, it merely requires he physically surrender pre-existing documents.[12]

But the Court in *Fisher* created an exception to this principle: if the very act of producing the document would itself be testimonial (and incriminating), then the suspect or witness may be able to assert a Fifth Amendment right and decline to produce the documents.[13] The Court said that the production can be testimonial if it communicates facts about the documents.[14] It might communicate that the documents exist, that the suspect possesses them, or that they are authentic.[15]

For example, if a subpoena required a defendant to produce any child pornography (hard copies) in his possession, the defendant would assert an act-of-production privilege. If he produced the documents, he would be communicating several incriminating facts: first, that he possessed the child pornography and second, that he knowingly possessed the images—both critical elements of the crime.

But *Fisher* was not done. It created an exception to the exception, roughly speaking. Under the foregone conclusion doctrine, the government can still compel production of the documents if it can show it already knows

10. Schmerber v. California, 384 U.S. 757, 765 (1966).
11. 425 U.S. 391 (1976).
12. *Id.* at 410–11.
13. *Id.* at 408.
14. *Id.* at 428–29 (Brennan, J., concurring).
15. *Id.*

they exist, the suspect possesses them, and that they are authentic.[16] Thus, if the government can show it already knows the defendant possesses particular images of child pornography, it can compel him to produce them; if it already knows he banks at a certain bank that regularly sends him monthly statements, it can demand those statements.[17] True, the production still communicates that he possesses them or that they are authentic, but for mysterious reasons the Court has determined that this production no longer counts as "testimonial"[18] under the Fifth Amendment when the government already knows the information that would be communicated by the production. The facts communicated by the production do not materially add to the government's case against the defendant.[19]

B. The Central Flaw

But these doctrines suffer from a fundamental flaw. Ordinary testimony involves a person communicating facts through language, using arbitrary sounds that the witness and the listeners intend and understand to be communicative. When a person utters the sound "yes," or even just nods her head in response to a question, she intends listeners to take these symbols to mean "yes" and not, for example, simply stretching her neck.[20] Ordinary testimony in this way is similar to acts deemed symbolic speech under First Amendment cases, which require that the person doing the act intend to communicate a particularized message and that others likely understand this message.[21]

But when we turn to a document production, the witness who produces the documents does not intend, *by that act*, to communicate any message at all. The person producing child pornography does not intend that act to be symbolically understood to mean "I possess these images." Rather, as an inadvertent by-product of the act, we may draw the ordinary inferences that the person possesses the files because that person was able to physically produce them. Or, if a person produces a bank account statement, we may infer the piece of paper is authentic because it came from the person's files.

---

16. *Id.* at 411.

17. United States v. Greenfield, 831 F.3d 106, 199–20 (2d Cir. 2016).

18. Courts appear to treat the foregone conclusion doctrine as measuring whether the act is testimonial. *Fisher*, 425 U.S. at 411 (When the foregone conclusion doctrine is met, the "question is not of testimony but of surrender.") (internal quotation and citation omitted); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014) (If the foregone conclusion test is met, the act "does not involve testimonial communication . . . ."). But Kerr argues the doctrine measures whether the facts communicated by the act are incriminating. Kerr, *supra* note 1, at 773. That debate probably does not matter here.

19. *Fisher*, 425 U.S. at 411.

20. *See generally* H.P. Grice, *On Meaning*, 66 PHIL. REV. 377 (1957). My distinction here rests very loosely on Grice's distinction between natural meaning—red spots "mean" measles—and non-natural meaning that occurs with language or other communication often based on arbitrary symbols. His explication of language involves a more complex set of intentions, of course.

21. Texas v. Johnson, 491 U.S. 397, 404 (1989).

The act of producing documents is thus not testimonial or communicative in the ordinary way.[22] As a result, courts must perform a nearly impossible task: determine what message the act of production, or the entering of a password, implicitly communicates without the normal or principled way to measure what a message means—speaker intent.

II. Devices

In applying the act of production doctrine, courts must assess what testimony is implicit in producing certain documents. As Kerr correctly summarizes, they usually assess whether the facts communicated are at issue in the case and add to the government's sum total of already existing evidence against the person—or as Kerr puts it, give the government a "prosecutorial advantage."[23] Producing a hard copy of child pornography would meet this test because it implicitly and directly communicates possession of the child pornography and likely knowing possession—both central elements of the crime.

The argument among courts, and between my view and Kerr's, centers on how we apply this accepted act of production doctrine to digital devices. Kerr argues that the opening of a device communicates one fact only: the fact that the person knows the password. True, this is one fact that is revealed, but not the only fact. The use of a password to open a device also communicates that the device likely belongs to the person and that the person possesses, perhaps knowingly, the files on the device.

The difference in what messages get communicated plays out in determining how the government may satisfy the foregone conclusion doctrine. If the only message communicated is knowledge of the password, then Kerr is right: the government need only show the person knows the password. If, however, the act of opening the device also communicates that the person likely owns the device and the files on it, then the government must show that it already knows of and can identify with reasonable particularity the actual files it seeks, or at least a class of files such as bank records for a particular account—a higher burden.

I will try to show Kerr is wrong here from two different approaches. First, I will simply apply the analogy to document productions in a somewhat mechanical way to show that courts should require the more robust showing to satisfy the foregone conclusion doctrine. I will then address the more fundamental question: what message does a person implicitly communicate in entering a password to open a device?

---

22. Kerr writes that the act of production communicates implicitly the same way raising a hand does to answer yes in response to a question. They are not analogous, however. In raising a hand, the person intends that act to count as a "yes" and intends the listener to see it that way. A person responding to a document production does not similarly intend the act of production to symbolically represent any message.

23. Kerr, *supra* note 1, at 774.

A. The Analogy Mechanically Applied

First, consider how the analogy applies literally. In a document production, the *act* is the physical act of handing over the documents. Assume this act tacitly communicates incriminating facts about possession, etc. A court would next decide whether the foregone conclusion doctrine would nevertheless allow the compelled production. Note that the foregone conclusion doctrine applies not to the act but to the documents ultimately produced. Does the government already know they exist, the suspect possesses them, and that they are authentic; in addition, can the government identify the documents with reasonable particularity? If not, the foregone conclusion doctrine does not apply, and the suspect can withstand production.

When we apply this analogy to a device, the outcome seems clear. Entering the password to open the device is analogous to the physical act of handing over the papers. The files on the device are analogous to the documents produced. Therefore, the foregone conclusion doctrine should apply to the files on the device. Can the government show it already knows they exist and the defendant possesses them?

But Kerr applies the analogy differently. True, he treats the act as entering the password.[24] But he treats the actual password as analogous to the files sought, therefore applying the foregone conclusion test to the password only. But his approach is not analogous. First, the abstract information of the password in the person's head is not the thing produced. It's not a thing at all, and it's not produced: we've stipulated that the person enters the password such that the government does not learn it. Rather, the things produced are the files on the device. Second, if the password were considered the thing produced, that would violate the Fifth Amendment because then the government would be compelling the person to reveal the password from their head—even Kerr concedes that we cannot compel the password itself from a person's head.

What matters in the act of production is the link between the act and the documents. In producing the documents, the pure physical act testifies *about* the documents. The person implicitly communicates he possesses them and that they are authentic. The act of production doctrine *links* the act to the documents, and the foregone conclusion doctrine relies for its central premise upon this link.

B. What Does the Act of Opening Communicate?

Moving beyond this more literal view of the analogy to the particulars, we can see that the same implicit testimony occurs in each situation as well. When a person opens her device, she implicitly communicates that she

24. *See* Kerr, *supra* note 1, at 778–79.

possesses the files on the device.[25] This follows quite directly: if she can open the device, it is likely—though not certainly—hers. If it is hers, the files on it are likely hers, and she therefore likely possesses them and knowingly possesses them. Of course, her opening a device may not prove beyond all doubt that she knowingly possesses the files on the device, but evidence need not enjoy this level of certainty. It need only make a material fact more likely.[26]

Kerr argues, by contrast, that knowledge of the password is the only actual testimony contained in the act of entering a password. He argues that other supposed communications, such as control of the device or possession of the files, are mere inferences from the testimony that therefore do not count as the testimony itself. He analogizes to ordinary testimony: if a person testifies she was at the scene of the crime, we may be able to infer she committed the crime, but she has not actually testified that she committed the crime.

But the problem with the act of production or the act of opening a device is that this type of tacit testimony differs fundamentally from ordinary testimony, and we therefore cannot analogize to it the way Kerr has done. Unlike ordinary oral testimony, for act-of-production testimony, *all* testimonial aspects of the act are inferences.[27] As noted above, we cannot look to the person's intent to determine the facts that count as communicated as part of the act because the person does not intend, by her act, to communicate any message at all.

If we cannot look to the message intended by the person producing documents, or entering a password, how can we decide which tacit or inferential messages count as sufficiently connected to the act to be testimonial aspects of that act? Kerr appears to answer this question when he notes that entering a password to open a device does not *necessarily* mean the device belongs to that person. From this we may infer that Kerr would apply the following rule: the act of entering a password implicitly communicates as testimony only those facts that are directly implicated, or that are communicated with certainty, with such certainty that the act is almost equivalent to the inference. Entering a password to open a device *equals* knowledge of the password, he might argue, whereas the same act merely implies the likelihood that the person owns the device and possesses its files.

This rule may have superficial appeal, but it does not work in the end. First, it violates the ordinary principles of evidence law, which draws no

25. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014) (By entering an encryption key, "the defendant implicitly would be acknowledging that he has ownership and control of the computers and their contents.").

26. FED. R. EVID. 401.

27. Doe v. United States, 487 U.S. 201, 208 (1988) (demonstrating that the act of production is an "implicit statement").

distinction between direct and circumstantial evidence.[28] If a person opens a device, we can infer she owns it, whether we denominate that act direct or circumstantial evidence.

But more important, the act-of-production cases themselves make clear that we must make inferences to glean the facts implied by the act of production—indeed, the entirety of the testimonial character of the act of production is one giant inference.[29] There is no core of testimony plus other facts that are mere inferences—as with ordinary spoken testimony. As the Court noted in *Doe v. United States*,[30] the act is testimonial "because it might entail implicit statements of fact."[31] Our question is simply which inferences are we to count as implicit assertions that accompany the act.

If a person produces bank documents, for example, we can infer those documents are authentic under the rules of evidence through two avenues of inference: first, if the person produced them in response to a request for one's bank documents, then they are likely that person's bank documents because the person believes they are.[32] Second, the mere fact, aside from the producer's belief, that the documents came from the defendant's files tends to show they are authentic,[33] just as they would be authenticated if the government merely seized them from his files.[34]

Both of these avenues to infer the documents are authentic represent indirect inferences that are not 100% certain. A person who produces a financial document in response to a subpoena may well be overinclusive whether from caution or laziness; document productions can be famously large and sometimes even deliberately padded. A person may deliberately or inadvertently produce financial documents that are actually those of her spouse or her client. If a prosecutor at trial sought to prove a particular document was authentic merely because the person produced it, a jury could find this is not enough evidence to find the document authentic; the defendant could say, "Well, I produced that by mistake, but it's not my bank account." In other words, producing the document tends to authenticate it but does not *equal* authenticating it. Kerr's rule for what counts as testimonial, and what counts as a mere inference, does not work when applied to ordinary act-of-production cases and therefore should not be applied to passwords.

---

28. *E.g.*, Desert Palace, Inc. v. Costa, 539 U.S. 90, 100 (2003).

29. *E.g.*, United States v. Hubbell, 530 U.S. 27, 37 (2000) ("implicitly communicate" statement of fact).

30. 487 U.S. 201 (1988).

31. *Id.* at 208.

32. Fisher v. United States, 425 U.S. 391, 412 n.12 (1976).

33. *E.g.*, United States v. Hubbell, 167 F.3d 552, 554 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000) (distinguishing between facts communicated via producer's beliefs and those simply communicated by the act itself and recognizing both as protected by the act of production doctrine). Kerr suggests that the act of production doctrine recognizes facts communicated about or via the producer's belief's only.

34. Burgess v. Premier Corp., 727 F.2d 826, 835 (9th Cir. 1984).

C. We Must Infer Even Knowledge of the Password

But even were we to accept Kerr's rule that the testimonial aspect of opening a device can involve only some kind of direct or immediate inference, that would not change matters. After all, if a person opens a device, we must still *infer* that the person knew the password, an inference that is far from certain or equivalent to the act. After all, the person may *not* have known the password, especially depending upon how we define the act compelled.

If we define the act as simply opening the device,[35] then this act certainly does not equal knowing the password. After all, the person may have opened the device with facial recognition, and no one would be able to tell because the government isn't allowed to watch her open it by stipulation (to prevent it from learning any password that has been entered). Or the device may not have a password, and it may simply have opened to the touch, the police having neglected to try this.

If we define the act more narrowly as entering the password, even here we must draw inferences. If the person enters numbers and the device opens, even that does not mean the person knows the password because she may have guessed it. Entering the password and opening the device does not *equal* knowing the password.[36]

Knowledge of the password requires inferences for another, more basic reason. The actual act compelled is simply entering some numbers or letters; from this act alone we cannot infer the person knows the password because those numbers might not open it. Only if the act succeeds, and the device opens, can we infer, working backwards, that the person must have known the password, again, assuming she did not guess it. Thus, entering the password does not *equal* knowing it; we must infer that fact from subsequent events. The inference is sound, of course, but an inference nonetheless.

Kerr's rule affords no reason to think that the inference of ownership or possession is any less direct or certain than the inference that the person knows the password. In almost all cases, at least with personal devices such as a smartphone, a person's ability to open the phone will be very powerful evidence of *both* facts: that she knows the password and that the device is hers. Any differences will "go to the weight" of the evidence, as judges are fond of saying. The differences are not fundamental enough to rank one inference as equivalent to the testimony and another as a simple inference from the testimony.

When we examine the act of opening a device closely, we see that the facts it communicates confirm the superficial application of the analogy to

---

35. *See, e.g.*, United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *1 (N.D. Cal. Apr. 26, 2018) (describing the compelled act as decrypting the device, rather than entering a password).

36. Even under Kerr's test, the government must show the person knows the password before she enters it.

the act of production; under both approaches, the act implicitly communicates ownership or control of the device and files on it, and the government should have to show, under the foregone conclusion doctrine, that it knows the person possesses these particular files, or class of files, and can identify them with reasonable particularity. Even then, the government should be entitled to those files only.[37]

III. What is the Best Rule Normatively?

Kerr wisely concludes his article by stepping back from the technical aspects of the act of production doctrine to argue that his rule is also the best rule normatively. Relying on his earlier "equilibrium theory," he argues that digital devices that encrypt and lock have given individuals new, unprecedented powers to hide evidence in a criminal case.[38] Strong encryption, after all, can make it impossible for the police, even with a warrant, to obtain relevant data, absent a workaround. Affording law enforcement relatively easy access to this data simply restores the ordinary balance between government and citizen.

This argument might work better if current Fourth Amendment doctrine were not so lacking. In other words, once a suspect has been compelled to open a device, the government may essentially search anywhere, every file and folder, every deleted file, metadata, location data, use data, and data we may not even realize our phones gather and keep. Current Fourth Amendment case law reads the warrant clause to impose very weak limits on obtaining a warrant and virtually no limits on the resulting search.

As a result, allowing law enforcement such easy access to devices under Kerr's rule does not restore some pre-existing status quo or ideal balance. Rather, it shifts to the government an unprecedented ability to scour very personal and private data that did not even exist twenty years ago. When we read the Fourth and Fifth Amendments together, many of us would prefer a more demanding rule: the government must show that the defendant possesses the documents it seeks and be able to identify those documents with reasonable particularity before it can compel a person to enter a password.

37. *See* Sacharoff, *supra* note 3, at 208.

38. *See* Kerr, *supra* note 1, at 794–96.