DECRYPTING THE FIFTH AMENDMENT: THE LIMITS OF SELF-INCRIMINATION IN THE DIGITAL ERA

Vivek Mohan & John Villasenor[*]

Technology has outgrown the Supreme Court's Fifth Amendment jurisprudence. This creates two distinct but related challenges. First, the scope of the "foregone conclusion" doctrine, which was originally formulated to address act-of-production issues for paper documents,[1] is ripe for review and clarification now that documents are almost always digital and often encrypted. Second, the question of what constitutes a "testimonial act" must be revisited to proactively ensure that the Fifth Amendment privilege against self-incrimination is not eviscerated by emerging technologies.

The Supreme Court articulated the foregone conclusion doctrine in 1976 in *Fisher v. United States*[2] and revisited it a quarter of a century later in *United States v. Hubbell*.[3] In neither case was the Court asked to consider the dizzying array of complex mechanisms available today to store and access electronic information.

In the last three years, circuit and district courts drawing their authority from *Fisher* and *Hubbell* have produced inconsistent rulings regarding the extent of the Fifth Amendment privilege against self-incrimination with respect to encrypted digital documents.[4] The question of whether a finger-swipe gesture used to unlock a smartphone is a testimonial act has also become important. A circuit split on these critically important components of criminal procedure

---

* Vivek Mohan is a fellow at the Harvard Kennedy School and a former attorney for Microsoft. John Villasenor is a nonresident senior fellow at the Brookings Institution and a professor of electrical engineering at UCLA. The authors thank Kiel Brennan-Marquez and Nabiha Syed for providing comments on an earlier draft.

1 *See* United States v. Hubbell, 530 U.S. 27, 36–37 (2000) (explaining that "the act of producing documents in response to a subpoena may have a compelled testimonial aspect").

2 425 U.S. 391, 411 (determining that the "existence and location" of the documents in question were a "foregone conclusion" and thus did not implicate any Fifth Amendment privileges).

3 530 U.S. at 44 (citing *Fisher*, 425 U.S. at 411) (considering the application of the foregone conclusion doctrine).

4 *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010); *In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009).

is likely to occur in the near future. When presented the opportunity, the Supreme Court should clarify the contours of the foregone conclusion doctrine and the scope of testimonial acts in the digital era.

I. INTRODUCTION

The Fifth Amendment guarantee that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself,"[5] as with almost all constitutional text, has a long and distinguished line of jurisprudence that has shaped the contours of the privilege. The foregone conclusion doctrine, originally articulated by the Supreme Court in 1976, identified conditions under which compelled production of documents does not implicate the Fifth Amendment.[6] The doctrine turns directly on the distinction between testimonial and non-testimonial evidence[7]—a distinction that has become much more challenging in a world in which people interact with electronic information in increasingly varied ways. In addition, technological advancements that offer the prospect of being able to infer—and in some cases even directly observe—thought processes raise difficult questions of the scope of the Fifth Amendment protection.

In short, in an era when documents are almost always electronic, often encrypted, and increasingly stored in the "cloud," the current framework with respect to compelled production is inadequate to address the complex range of scenarios that are starting to arise. Today's courts thus face the unenviable challenge of engaging in contortions to fit the square peg of contemporary encryption and document storage methods into the round hole of existing Fifth Amendment doctrine. This is yet another manifestation of the ability of technological advancements to reshape the fundamental contours of constitutional protections.

We describe some key challenges that technological advances pose to the Fifth Amendment with respect to the act of production doctrine, and propose a set of prescriptive solutions that are better matched to today's technologies. In particular, we argue that courts have misapplied the Supreme Court's ruling in *Hubbell* by reading in a requirement of "location" rather than "possession."

It is important to note that we focus our analysis on circumstances where the government has an established right, through a validly executed search warrant, or other exception, such as a routine border

5 U.S. CONST. amend V.

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

7 *Id.* at 408–11.

search,[8] to conduct a search or seizure. We do not address Fourth Amendment considerations, which raise their own separate and important issues in light of technological advances.

II. THE FOREGONE CONCLUSION DOCTRINE AND TESTIMONIAL ACTS

The Supreme Court has prefaced its inquiries into the Fifth Amendment by explaining that the oft-repeated term "privilege against self-incrimination" is "not an entirely accurate description of a person's constitutional protection against being 'compelled in any criminal case to be a witness against himself.'"[9] The limits of the privilege extend only to the compulsion of "incriminating communications . . . that are 'testimonial' in character."[10] As the Court wrote in 1911, compelling a defendant to "yield possession of property that he no longer is entitled to keep" is a question "not of testimony but of surrender."[11]

Perhaps the test that most defines modern conceptions of the privilege comes from the 1957 case *Curcio v. United States*.[12] In 1956, Joseph Curcio, who was then the secretary-treasurer of Local 269 of the International Brotherhood of Teamsters in New York, was subpoenaed to produce the union's records.[13] During testimony before a grand jury, he stated that the records were not in his possession and then invoked his right against self-incrimination in refusing to state who held them or where they were stored.[14] Upon his refusal, the District Court found him guilty of criminal contempt and ordered him incarcerated.[15] The Second Circuit affirmed the conviction, but the Supreme Court overturned, holding that forcing a custodian to "testify orally as to the whereabouts of nonproduced records *requires him to disclose the contents of his own mind.* He might be compelled to convict himself out of his own mouth. That is contrary to the spirit and letter of the Fifth Amendment."[16]

The "contents of . . . mind" language from *Curcio*[17] provided the basis for Justice Stevens' oft-cited 1988 dissent in *Doe v. United States*,

---

8 *See* United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (stating that conducting a routine border search does not require any basis for suspicion).

9 United States v. Hubbell, 530 U.S. 27, 34 (2000).

10 *Id.*

11 *In re* Harris, 221 U.S. 274, 279.

12 354 U.S. 118.

13 *Id.* at 119.

14 *Id.*

15 *Id.* at 121.

16 *Id.* at 128 (emphasis added).

17 *Id.*

where he wrote that a defendant may "be forced to surrender a key to a strongbox containing incriminating documents," but could not "be compelled to reveal the combination to his wall safe—by word or deed."[18] The majority incorporated this language in *dicta*.[19]

A. The Doctrine Articulated: Fisher

In the 1976 case *Fisher v. United States*, attorneys refused to produce taxpayer documents sought by the IRS, citing their client's Fifth Amendment privilege.[20] The Supreme Court ruled for the IRS, and in its holding the Court articulated what has become known as the foregone conclusion doctrine, explaining that "the act of producing [the papers]—the only thing which the taxpayer is compelled to do—would not itself involve testimonial self-incrimination."[21] The Court held that the government can compel production when the "existence and location [of documents] are a foregone conclusion and [the defendant] adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[22]

B. Hubbell*: The Last Word from the Supreme Court*

In the 2000 case *United States v. Hubbell*, a grand jury subpoenaed documents from an official who refused to comply, asserting his Fifth Amendment privilege.[23] The district court ordered the documents to be produced, and granted "use and derivative-use" immunity under 18 U.S.C. § 6002.[24] In a subsequent action challenging the use of these documents in a criminal case on Fifth Amendment grounds, the Supreme Court found Hubbell's production of documents to be a testimonial act, relying in large part on the lack of *a priori* government knowledge of the subpoenaed documents.[25]

The Court wrote that "the act of producing documents in response to a subpoena may have a compelled testimonial aspect," as "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena."[26] The Court

---

18 487 U.S. 201, 219.
19 *See id.* at 210 n.9.
20 425 U.S. 391, 393–95.
21 *Id.* at 411.
22 *Id.* (citing *In re* Harris, 221 U.S. 274, 279 (1911)).
23 530 U.S. 27, 31.
24 *Id.* at 38 (citing Kastigar v. United States, 406 U.S. 441 (1972)).
25 *Id.* 41–43.
26 *Id.* at 36, 43 (citing Curcio v. United States, 354 U.S. 118, 128 (1957); Doe v. United States, 487 U.S. 201, 210 (1988)).

also noted that the act of production and the custodian's compelled testimony as to whether all documents demanded have been produced "certainly communicate information about the existence, custody, and authenticity of the documents."[27]

It has been observed that the *Hubbell* Court may have gone farther than merely contrasting the facts in *Hubbell* from those in *Fisher*, reading the case as expressing doubt as to the prudential applicability of the foregone conclusion doctrine.[28] The *Hubbell* Court lamented the lack of clarity in the foregone conclusion doctrine, and in *dicta* established the vague standard that would be applied by lower courts in subsequent years:

> Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it. While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent.[29]

C. Ponds *and the Reasonable Particularity Standard*

Lower courts have applied a standard requiring a showing of "existence, custody, and authenticity," drawing authority from the Court's language in *Hubbell*.[30] The Supreme Court heard *Hubbell* on *certiorari* from the D.C. Circuit, and affirmed the decision of the lower court.[31] However, the Supreme Court did not adopt the exact wording of the D.C. Circuit, which had suggested that for a response to a subpoena request to be non-testimonial in nature, the government must "'establish[] its [pre-subpoena] knowledge of the existence, possession, and authenticity of the subpoenaed documents with '*reasonable particularity*'' such that 'the communication inherent in the act of production can be considered a foregone conclusion.'"[32] Instead, the Supreme Court left *Hubbell* with the broader "existence, control, and authenticity" standard, declining to adopt the proposed standard of "reasonable particularity."

---

27 *Id.* at 37.

28 *See* Mark A. Cowen, Note, *The Act-of-Production Privilege Post-*Hubbell*:* United States v. Ponds *and the Relevance of the "Reasonable Particularity" and "Foregone Conclusion" Doctrines*, 17 GEO. MASON L. REV. 863, 873 (2010).

29 *Hubbell*, 530 U.S. at 44–45.

30 *See id.* at 37, 41.

31 *See id.* at 46.

32 United States v. Ponds, 454 F.3d 313, 324 (D.C. Cir. 2006) (emphasis added) (quoting United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999)).

Despite the Supreme Court's actions in *Hubbell*, in the 2006 case *United States v. Ponds*, the D.C. Circuit nevertheless decided to readopt the "reasonable particularity" standard it had proposed in its own *Hubbell* decision.[33] The D.C. Circuit justified its decision to do so by noting that its earlier decision in *Hubbell* had not been overturned, and further, that this standard had been adopted by the Ninth Circuit.[34] It has since been adopted by the Eleventh Circuit as well.[35]

D. Defining the Boundaries of "Testimony"

In considering the limits of behavior that constitutes testimonial communication, the Court held in 1966 that the Fifth Amendment "offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."[36] The Court in *Hubbell* pointed to a long line of case law that establishes that a criminal suspect may be

> [C]ompelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief.[37]

However, commentators have noted the long history of inconsistency and unpredictability in divining what qualifies as a testimonial act.[38] For example, Allen and Mace have noted that attempts to reconcile the use of machines to interpret non-vocal physiological responses to stimuli with existing "testimonial" doctrine "feeds the sense that there is a conceptual hole at the middle of the Fifth Amendment."[39]

III. COMPELLED DECRYPTION: RECENT RULINGS

Encryption poses clear challenges for applying the foregone conclusion doctrine. Today's encryption technologies are sufficiently advanced to effectively block any attempt at a brute force attack: While

---

33 *Id.* at 320–21.

34 *Id.* (citing *In re* Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004)).

35 *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012).

36 Schmerber v. California, 384 U.S. 757, 764 (1966).

37 United States v. Hubbell, 530 U.S. 27, 35 (2000) (citing Pennsylvania v. Muniz, 496 U.S. 582, 594–98 (1990)).

38 *See* Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243 (2004).

39 *Id.* at 249.

in theory it is possible to attempt every possible password, the number of possible combinations means that such an attack would stand almost no chance of succeeding in any reasonable time frame. This was explicitly noted by prosecutors in *In re Boucher*, who had seized a laptop computer but were unable to decrypt its contents: "The government is not able to open the encrypted files without knowing the password. In order to gain access . . . the government is using an automated system which attempts to guess the password, a process that could take years."[40]

An additional complication is that encryption can be used to scramble the entire contents of a hard drive or other storage device, making it impossible to distinguish ones and zeros that might represent a document from ones and zeros that are nothing but empty storage space.[41] This aspect of encryption is unique to digital storage media. Encryption, of course, is not new, having played a role in historical events such as the failed 1586 plot to assassinate Queen Elizabeth and place Mary Queen of Scots on the throne[42] and the German Enigma machines used during World War II.[43] But an encrypted paper document is typically identifiable as exactly that, and there is no difficulty in distinguishing it from the empty space that may sit above it in a storage box. By contrast, an encrypted digital document can be impossible to separate from its digital surroundings, regardless of whether those surroundings contain other documents or the digital equivalent of empty space. This raises obvious challenges with respect to establishing the existence and location of documents as required by the foregone conclusion doctrine.

In various district courts around the country, we have seen judges struggle to apply the Court's "existence, custody, and authenticity" and "foregone conclusion" standards in cases where the government requires a password to access encrypted files on a digital storage device that the government has in its possession.

---

40 No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *5–6 (D. Vt. Feb. 19, 2009).

41 See, for example, TrueCrypt: "Until decrypted, a TrueCrypt partition/device appears to consist of nothing more than random data (it does not contain any kind of 'signature'). Therefore, it should be impossible to prove that a partition or a device is a TrueCrypt volume or that it has been encrypted (provided that the security requirements and precautions listed in the chapter *Security Requirements and Precautions* are followed)." *Plausible Deniability*, TRUECRYPT, http://www.truecrypt.org/docs/?s=plausible-deniability (last visited Oct. 5, 2012).

42 *See* SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 1–3 (1999).

43 *See id.* at 181.

A. Kirschner

In *United States v. Kirschner*, the Eastern District of Michigan held in a 2010 ruling that a grand jury subpoena, issued without immunity, requiring the defendant to divulge the password to decrypt an encrypted hard drive, would violate his Fifth Amendment privilege.[44] Noting that "the government is not seeking documents or objects—it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password—that will be used to incriminate him," the court quashed the subpoena, "thereby protecting [the Defendant's] invocation of his Fifth Amendment privilege against compelled self-incrimination."[45]

B. Boucher

In *In re Boucher*, a government agent examined, with the defendant's assistance, an encrypted drive on a laptop and ascertained that it contained incriminating files.[46] The defendant later sought to invoke his Fifth Amendment privilege in refusing subsequent requests to divulge his password.[47] The District of Vermont, in rejecting the assertion of the privilege, held in 2009 that "providing access to the unencrypted [] drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information."[48] Additionally, the court noted that the "act of producing an unencrypted version of the [] drive likewise is not necessary to authenticate it. He has already admitted to possession . . . and provided the Government with access . . . ."[49]

C. Fricosu

In *United States v. Fricosu*, the government recorded conversations between the defendant and a third party that suggested that encrypted files on a seized laptop contained incriminating files.[50] The case was heard in the District of Colorado, which as part of the Tenth Circuit has not adopted the reasonable particularity standard. In January 2012, the District of Colorado ordered the defendant to supply

44 823 F. Supp. 2d 665.
45 *Id.* at 669.
46 No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *4–5 (D. Vt. Feb. 19, 2009).
47 *Id.* at *2.
48 *Id.* at *9 (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).
49 *Id.* at *9–10.
50 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012).

the password to decrypt the laptop under the foregone conclusion doctrine, arguing that "[t]he fact that [the government] does not know the specific content of any specific documents is not a barrier to production."[51] While the case might have received further attention at the circuit level, the issue of compelled decryption of the seized laptop was rendered moot when the government was able to decrypt the drive without the defendant's assistance.[52]

D. The Eleventh Circuit

One of the most expansive recent rulings to address compelled decryption was issued by the Eleventh Circuit in February 2012 in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*.[53] In October 2010, law enforcement agents pursuing a child pornography investigation tracked a Florida man suspected of sharing illegal images to a hotel room in California.[54] After obtaining a search warrant, they raided the room, seizing computers and hard drives with nearly five terabytes of total storage capacity.[55] However, they soon hit a roadblock: Portions of the hard drives had been encrypted and were unreadable without a password.[56] The suspect refused to decrypt the drives, and a federal district court in Florida held him in contempt and ordered him incarcerated.[57]

In February 2012, the Eleventh Circuit Court of Appeals overturned the contempt holding, ruling that the suspect's refusal was protected under the Fifth Amendment right against self-incrimination.[58] The court applied the *Ponds* "reasonable particularity" standard, noting that

> [I]f the Government is unaware of a particular file name, it still must show with some reasonable particularity that it seeks a certain file and is aware, based on other information, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic. Thus, although the Government need not know the name of a particular file or account, it still must be able to establish that a file or account, whatever its label, does in fact exist.[59]

---

51 *Id.* at 1237.

52 *See* David Kravets, *Constitutional Showdown Voided: Feds Decrypt Laptop Without Defendant's Help*, WIRED (Feb. 29, 2012, 5:17 PM), http://www.wired.com/threatlevel/2012/02/decryption-flap-mooted/.

53 670 F.3d 1335.

54 *Id.* at 1339.

55 *Id.*

56 *Id.*

57 *Id.* at 1340.

58 *Id.* at 1341.

59 *Id.* at 1349 (citation omitted).

IV. SHOULD "LOCATION" BE A PRONG OF THE FOREGONE CONCLUSION DOCTRINE?

Digital encryption raises, in a new context, the same two foundational issues—specificity of *a priori* government knowledge, and the bounds of testimony—that have underpinned much of the case law relating to the foregone conclusion doctrine: First, to what level of specificity must the government have knowledge regarding encrypted documents before it can compel decryption? And second, under what circumstances is the act of providing the government information that might help it decrypt documents testimonial?

A. Is "Reasonable Particularity" a Reasonable Standard?

The Ninth, Eleventh, and D.C. Circuits have adopted the "reasonable particularity" standard under the auspices of the "existence, custody, and authenticity" framework elaborated in *Hubbell*. Application of this framework would seem to indicate that absent external, prior verification of incriminating documents, as was the case in *Boucher*, the technological capabilities in commercially available encryption software present a nearly insurmountable hurdle for the government to use the foregone conclusion doctrine to compel decryption of an encrypted storage device.

However, it is not at all clear that the reasonable particularity standard will be adopted by the other circuits. It is even less clear that the "reasonable particularity" standard is the correct rule—either in terms of the Supreme Court's jurisprudence in *Hubbell* or in terms of current technologies. Given that the Supreme Court was specifically presented with the "reasonable particularity" standard in *Hubbell* and chose not to adopt it, there is a question as to whether its continued application at the circuit level is proper.

B. Clouding the Concept of "Location"

More fundamentally, the right question to ask may not be whether the location must be known with "reasonable particularity," but whether location is an appropriate test to apply at all. The term "location" suggests a specific, physically identifiable device or place that contains the documents in question. This is ill-matched to an environment for storing and exchanging documents that is increasingly based on cloud computing, which of course is designed in part to abstract away the need to know or track location.

Unsurprisingly, determining the location of a document stored in the cloud is difficult. A user of Google Docs or Amazon's cloud-based Simple Storage Service typically has no information regarding what

specific physical storage device is used to store his or her documents. In addition, in many cases the location of a document may be dynamic. A document can initially be stored in one place, and then repeatedly moved by a cloud service provider as part of a resource rebalancing process. The cloud service provider might sometimes choose to store multiple copies of a document, or to partition a single copy of the document into separately stored fragments. All of these actions would of course be invisible to the document owner.

Investigators aiming to identify the location of a particular document stored on the cloud would need to (1) determine the suspect's cloud service provider, (2) identify the location of the (likely encrypted) data controlled by the suspect, and (3) identify which subset of that data was associated with the desired document. Clearly, these steps would involve many hurdles.

It is also possible to envision ways for a document owner to use cloud computing in a manner intentionally structured to challenge the very concept of location. Consider, for example, software designed to take a single document, partition it into thousands of fragments, and store each of those fragments on a different peer-to-peer server somewhere on the Internet. There would not even need to be a single master map identifying the location of each fragment; that map itself could be stored in a distributed manner, or woven into the document's data fragments. To further complicate matters, software could be designed to automatically move the document fragments every few hours, or even every few seconds. The result would be a document stored on a literally global scale across a constantly shifting mosaic of servers.

What is the location of such a document that is, in a sense, both nowhere and everywhere? Clearly, it would be impossible for authorities to meet the *Ponds* standard of identifying the document's location to "reasonable particularity" when attempting to compel production. Even if authorities were somehow able to obtain a list of the relevant server locations at a particular snapshot in time, the list would be obsolete by the time they petitioned a court to compel production. Even in the absence of the "reasonable particularity" standard, the foregone conclusion doctrine's requirement with respect to "location" is clearly ill-suited for these types of scenarios.

It is tempting here to create a distinction between the Fifth Amendment as applied to the physical world from that as applied to the digital domain. However, creating one set of constitutional standards for digital or digitally stored information and another set of standards for the "physical world" is problematic for a number of reasons. Not only would this raise consistency issues, but there is also a threshold question of whether digital and physical domains can be

realistically distinguished. Digital information which exists at one or more locations unknown even to its owner does still physically reside on real storage devices—and as computers find their ways into heretofore unexpected aspects of our daily lives, proposing to distinguish physical and digital as separate domains for purposes of the foregone conclusion doctrine would be improper. The better approach is to update the doctrine so that it can be applied more ably to both domains.

C. Hubbell *and* Fisher *Reconsidered*

In that context, a closer reading of *Hubbell* is instructive. *Hubbell* did not codify an interpretation of the Constitution that would require the government to specify the "location," or "whereabouts," of information to fulfill the requirements of the foregone conclusion doctrine. Instead, the *Hubbell* Court expressed doubt that the government could fulfill the requirements of the foregone conclusion doctrine where it "has not shown that it had any prior knowledge of either the existence or the whereabouts"[60] of the documents.

The Court in *Hubbell* discussed the foregone conclusion doctrine in the *negative* and never expressly stated that both existence and location must be specified for the government to prevail when seeking to apply the foregone conclusion doctrine. Instead, the *Hubbell* Court repeatedly stated that the foregone conclusion doctrine is *inapplicable* when a defendant is compelled to provide information regarding the existence, possession (or control), or authenticity of documents.[61]

It is quite possible for the government to show knowledge of existence, possession, and authenticity without specifying the technologically problematic "location" of such information. Thus, there is a path that is fully consistent with *Hubbell* to removing the explicit requirement of location and, along with it, the question of whether location must be known with reasonable particularity.

It could be argued that *Fisher* gives more weight to location than *Hubbell*. Consider *Fisher*'s oft-cited holding that "[t]he 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."[62] However, the *Fisher* Court also stated that "[i]t is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testi-

60 United States v. Hubbell, 530 U.S. 27, 45 (2000).

61 *See id.* at 41, 43–45.

62 Fisher v. United States, 425 U.S. 391, 411 (1976).

mony within the protection of the Fifth Amendment."[63] In 1976, the concepts of "possession" and "location" of documents were far more closely intertwined than they are today, and the *Fisher* Court's apparent use of these terms in an interchangeable manner was understandable. *Fisher* can also be interpreted as conveying that the core concept is "possession"—which mapped in 1976 directly to location, but no longer does. To the extent that these readings as to whether location is an inescapable requirement of the foregone conclusion doctrine are potentially inconsistent, *Hubbell* must be given more weight as the more recent ruling.

V. FOREGONE CONCLUSION: AN UPDATED FRAMEWORK

Recent circuit cases on compelled decryption usually characterize the three prongs of the foregone conclusion doctrine as existence, location, and authenticity. However, we believe that replacing "location" with "possession" or "control" is the correct reading of *Hubbell*. If the government is able to establish that a suspect possesses a particular file, the suspect should not then be able to effectively circumvent government efforts to obtain the document by simply using encryption to bury it in a mass of indistinguishable ones and zeros on a hard drive. Similarly, a document placed in the cloud, either in encrypted form or not, remains within the possession of the suspect.

The "existence" prong remains an appropriate component of the foregone conclusion doctrine. However, establishing that it is met can be difficult with digital documents. It will often be possible for the government to prove, through records subpoenaed from Internet or wireless service providers, that a suspect has downloaded a particular document. However, while this shows that the document existed (and was possessed by the suspect) at some point in the past, it does not show that the document still exists.

In many digital environments, "deleting" a document does not actually overwrite it on a storage device. Instead, it typically frees the associated storage space so that it can be used to store new information. Whether and how quickly the original document data is actually overwritten with new data depends, of course, on many factors. From a purely technical standpoint, the document can reasonably be said to exist as long as it is recoverable.

How can the government show that a document that was downloaded one month, or one year, ago still exists? The government will almost never be able to prove the negative—i.e., that in the interven-

63 *Id.*

ing time the suspect did not delete and overwrite the relevant file. Forcing the government to provide that proof would be tantamount to putting nearly all encrypted digital documents beyond discovery. On the other hand, exposing suspects to compelled decryption just because they are known, at some potentially distant time in the past, to have received a particular document, puts far too much power in the hands of the government.

Between these two undesirable extremes there is a solution, though not a perfect one: The government must show that the documents in question did indeed recently[64] exist on media controlled by the suspect. Defendants ordered to decrypt the associated media get immunity for all documents that were not specifically identified in the government's showing of "existence." This would prevent government fishing expeditions to acquire previously unknown documents for use against the suspect.

VI. DOES TECHNOLOGY CHALLENGE THE BOUNDARIES OF WHAT IS TESTIMONIAL?

The issue of compelled decryption inevitably turns in large part on the question of what constitutes a testimonial act. While precedent clearly establishes that mere physical characteristics are not afforded the protections of the Fifth Amendment, emerging technologies increasingly blur the distinction between physical attributes or actions and assertions of fact or belief.

Courts generally agree that divulging a password constitutes a testimonial act. Conversely, it is clear that a thumbprint is clearly nontestimonial, and the Fifth Amendment would not block authorities from compelling a suspect to provide a thumbprint needed to unlock his or her computer. The image of a suspect's face is also nontestimonial. Wireless device maker HTC was recently granted a patent for the use of face recognition in unlocking a computing device such as a smartphone.[65] The owner of such a phone, if it were seized in a future criminal investigation, could not prevent authorities from using the image of his or her face to unlock it.

---

64 There is not necessarily an ideal answer to the question of what, exactly, "recent" might mean. Leaving the time duration unspecified creates the potential for governmental abuse. On the other hand, picking a particular number of days, weeks, or months would create what amounts to a very short statute of limitations, which would be problematic for other reasons, including the likely creation of software specifically designed to circumvent the time limit. In our view, this should be subject to review by a trial court to evaluate in the context of the alleged duration of the criminal activity.

65 *See* Vlad Bobleanta, *HTC Wins Patent for Face Unlock*, UNWIRED VIEW (Apr. 4, 2012), http://www.unwiredview.com/2012/04/04/htc-wins-patent-for-face-unlock/.

A. Are Gestures Testimonial?

Gestures, however, present a more complex case. For example, consider the "pattern lock" used in place of a traditional alphanumeric password to secure some smartphones. These phones are unlocked when their owner traces a finger over the screen in a specific, personalized pattern. The pattern is chosen by the owner when he or she first acquires and configures the smartphone and is not generally known to the manufacturer of the phone or to the associated wireless service provider.

Pattern locks have already become an issue in criminal investigations. In January 2012, FBI agents seized a phone secured by a pattern lock from a suspect in a San Diego-area prostitution investigation.[66] As detailed in an FBI affidavit, technicians "attempted to gain access to the contents of the memory of the cellular telephone in question, but were unable to do so."[67] The affidavit further explains:

> Failure to gain access to the cellular telephone's memory was caused by an electronic "pattern lock" programmed into the cellular telephone. A pattern lock is a modern type of password installed on electronic devices, typically cellular telephones. To unlock the device, a user must move a finger or stylus over the keypad touch screen in a precise pattern so as to trigger the previously coded un-locking mechanism. Entering repeated incorrect patterns will cause a lock-out, requiring a Google email login and password to override. Without the Google email login and password, the cellular telephone's memory can not be accessed.[68]

Having failed to identify the pattern needed to unlock the phone, federal investigators sought, and were granted, a warrant ordering Google to provide the login and password that would, in effect, circumvent the pattern lock.[69]

Despite that workaround, it appears that the disclosure of a pattern is a testimonial act, as it "requires [the defendant] to disclose the contents of his own mind."[70] The government should have no more ability to compel the phone owner to disclose the pattern than it would have to compel disclosure of an alphanumeric password.[71]

---

66 See Affidavit in Support of Search Warrant Application at 4–5, No. 3:12-mj-00882-NLS (S.D. Cal. Mar. 9, 2012), *available at* http://www.wired.com/images_blogs/threatlevel/2012/03/gov.uscourts.casd_.378626.1.0.pdf (last visited Oct. 5, 2012).

67 *Id.* at 7.

68 *Id.*

69 *See* Application and Affidavit for Search Warrant, No. 3:12-mj-00882-NLS (S.D. Cal. Mar. 9, 2012), *available at* http://www.wired.com/images_blogs/threatlevel/2012/03/gov.uscourts.casd_.378626.1.0.pdf (last visited Oct. 5, 2012).

70 Curcio v. United States, 354 U.S. 118, 128 (1957).

71 However, unlike a password, the pattern may be discernible without ever consulting the smartphone owner, especially if the phone has been unlocked hundreds of times. Much as a dirt path is formed in a grassy field that is repeatedly traversed in the same way, using

While courts have addressed the testimonial nature of these technologies on an *ad hoc* basis, emerging technologies present broader constitutional challenges that are not so easily reconciled.

B. Keeping Secrets from Big Brother: Technologies That Can Read Our Thoughts

It is tempting to make the distinction that physically measurable biometric attributes (fingerprints, iris and retina attributes, the shape of someone's face, etc.) are non-testimonial, while interactions with a device (entering a password, using a finger to trace the pattern in a pattern lock) involve testimonial information. But this distinction faces challenges given the increasing ability to obtain measurements conveying the contents of a person's mind. In fact, the entire concept of protecting the contents of a person's mind rests on the assumption that those contents must be voluntarily disclosed before others can know them. Current technology trends call the strength of that assumption into question.

For example, eye-tracking uses images from one or more cameras to capture subtle changes in the movements and structure of our eyes. Researchers in the United States and the United Kingdom have mapped the correlation between blink rates,[72] pupil dilation,[73] and deception. The Department of Homeland Security has been using eye-tracking technology in a "pre-crime" program aimed at identifying criminals before they act.[74] The DHS program, known as Future Attribute Screening Technology, is designed to analyze images acquired at airport security checkpoints to measure eye movement, position, and gaze (as well as heart rate, respiration, and facial expression) to identify behavior deemed suspicious.[75]

Eye-tracking and related methods could allow investigators to ask questions that lead to information about the contents of a suspect's

---

a pattern on a smartphone could create subtle evidence of wear on the screen that could be identified using advanced imaging and measurement techniques. These measurements, of course, would not implicate the Fifth Amendment. Thus, once the phone is well-worn enough so that the pattern can be ascertained by physical analysis of the phone, the pattern is in some sense both like a combination to a lock and a key to a strongbox: It is the contents of the phone owner's mind, but it is also ascertainable from physical attributes of the phone that can be measured without the suspect's participation.

72 *See* Lucy Cockcroft, *Liars are Exposed by Blinking*, THE TELEGRAPH (Aug. 20, 2008, 8:32 AM), http://www.telegraph.co.uk/news/2589073/Liars-are-exposed-by-blinking.html.

73 *See You Can't Hide Your Lyin' Eyes*, UNIVERSITY OF UTAH (July 12, 2010), http://unews.utah.edu/news_releases/you-can039t-hide-your-lyin039-eyes/.

74 *See* Declan McCullagh, *Homeland Security Moves Forward with "Pre-Crime" Detection*, CNET (Oct. 7, 2011, 4:00 AM), http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/.

75 *See id.*

mind, even when he or she declines to provide a verbal answer. It is easy to envision a sort of "20 questions" approach designed to elicit information that might make a password easier to crack. For example, a suspect's reaction to questions such as "does your password have fewer than 10 characters?" or "does it contain any numbers?" might allow investigators to greatly narrow the set of possible passwords, thereby increasing their ability to access a secured device using a brute force search.

The end game for these sorts of approaches lies in technologies that quite literally measure the contents of a person's mind. Functional MRI (fMRI), which enables real-time measurement of localized activity within the brain, is starting to make this feasible.

In 2011, Princeton researchers demonstrated that it is "possible to generate *text* about the mental content reflected in brain images."[76] The researchers "found that they could confidently determine from an fMRI image the general topic on a participant's mind, but that deciphering specific objects was trickier."[77] For example, while today's fMRI methods might make it possible to determine that a person is thinking about a vegetable as opposed to a type of furniture, they are unable to identify which specific vegetable the person is visualizing. fMRI methods of the future will presumably allow more specificity.

The prospect that fMRI methods could be used to forcibly extract information from a person's mind is chilling. However, investigators clearly have the right to videotape an interrogation, and subsequently study the video for cues contained in eye movements and respiration. The use of cameras with sufficiently high resolution to discern pupil dilation and pulse rate is equally unlikely to be deemed unconstitutional.

At some point, however, government use of these newer technologies will run up against the Fifth Amendment. In the near future, fMRI technologies might enable the extraction of simple thoughts such as information relating to passwords. In our opinion, using fMRI methods to extract information raises questions both of the testimonial nature of the act and of compulsion.

Allen and Mace have argued that "testimony is the substantive content of cognition."[78] While this definition has not been adopted by the Court, the use of fMRI methods presents an eye-opening case

---

76 Francisco Pereira, Greg Detre & Matthew Botvinick, *Generating Text from Functional Brain Images*, FRONTIERS IN HUM. NEUROSCIENCE, Aug. 2011, at 1.

77 Morgan Kelly, *Word Association: Princeton Study Matches Brain Scans with Complex Thought*, PRINCETON UNIVERSITY (Aug. 31, 2011, 9:00 AM), http://www.princeton.edu/main/news/archive/S31/47/31I07/index.xml?section=topstories.

78 Allen & Mace, *supra* note 38, at 250 (internal quotation marks omitted).

study on the limits of the current definition of "testimony." Technologies such as fMRI call for outdated definitions of testimony to be clarified to fully encapsulate and protect the "contents of [our] mind."

In our opinion, not only must the definitions of testimony and cognition be linked, but suspects must also be able to positively assert their Fifth Amendment privilege against such invasive procedures. We suggest that the assertion of the privilege can be characterized as "positive" or "negative." In a "positive" framework, to protect the products of his or her cognition (the *Curcio* "contents of his mind"), a suspect has the right to affirmatively assert the privilege to stop the government from analyzing his or her brainwaves. In a "negative" framework, a suspect only has the right to refuse to use his or her volition to furnish the government with the "contents of his mind." Without linking testimony and cognition, he or she has no right to affirmatively stop the government from procuring those contents by other means; the use of emerging technologies to reverse-engineer thoughts would pose no Fifth Amendment problem.

VII. CONCLUSION

Properly bringing the foregone conclusion doctrine into the digital era is challenging but necessary; we believe that "location" is neither constitutionally required nor practically feasible as applied to the mechanisms commonly used to store and access documents today, and that "possession" is the correct standard to be applied. "Existence" remains an appropriate prong of the foregone conclusion doctrine, though there are new challenges to establishing it. As we have explained, it is important to ensure that suspects are protected from interpretations of "existence" that would open the door to fishing expeditions by the government. Additionally, while updating the definition of what constitutes a testimonial act presents challenges that have bedeviled the Court for many years, emerging technologies make this an issue in need of clarification.

In closing, we again emphasize a point made in the introduction—it is exceedingly difficult to unravel the tightly intertwined nature of the Fourth and Fifth Amendments and examine only one in a vacuum. However, we believe the foregone conclusion doctrine and the limitations on the definition of testimony present discrete—and pressing—opportunities for the Court to clarify Fifth Amendment doctrine so that it can be interpreted and applied in a manner more consistent with today's technologies.