670 F.3d 1335
United States Court of Appeals,
Eleventh Circuit.

In re GRAND JURY SUBPOENA DUCES TECUM DATED MARCH 25, 2011.
United States of America, Plaintiff–Appellee,
v.
John Doe, Defendant–Appellant.

Nos. 11–12268, 11–15421. | Feb. 23, 2012.

TJOFLAT, Circuit Judge:

This is an appeal of a judgment of civil contempt. On April 7, 2011, John Doe was served with a subpoena duces tecum requiring him to appear before a Northern District of Florida grand jury and produce the unencrypted contents located on the hard drives of Doe's laptop computers and five external hard drives.[1] Doe informed the United States Attorney for the Northern District of Florida that, when he appeared before the grand jury, he would invoke his Fifth Amendment privilege against self-incrimination and refuse to comply with the subpoena. * * *

On April 19, 2011, the U.S. Attorney and Doe appeared before the district court.[5] The U.S. Attorney requested that the court grant Doe immunity limited to "the use [of Doe's] act of production of the unencrypted contents" of the hard drives. That is, Doe's immunity would not extend to the Government's derivative use of contents of the drives as evidence against him in a criminal prosecution. The court accepted the U.S. Attorney's position regarding the scope of the immunity to give Doe and granted the requested order. The order "convey[ed] immunity for the act of production of the unencrypted drives, but [did] not convey immunity regarding the United States' [derivative] use" of the decrypted contents of the drives.

After the hearing adjourned, Doe appeared before the grand jury and refused to decrypt the hard drives. The U.S. Attorney immediately moved the district court for an order requiring Doe to show cause why Doe should not be held in civil contempt. The court issued the requested order, requiring Doe to show cause for his refusal to decrypt the hard drives. Doe, responding, explained that he invoked his Fifth Amendment privilege against self-incrimination because the Government's use of the decrypted contents of the hard drives would constitute derivative use of his immunized testimony, use not protected by the district court's grant of immunity.[6] An alternative reason Doe gave as to why the court should not hold him in contempt was his inability to decrypt the drives. The court rejected Doe's alternative explanations, adjudged him in contempt of court, and ordered him incarcerated. Doe now appeals the court's judgment.

* * * Part I briefly reviews the relevant factual background and procedural history of the

case. Part II discusses ***1339** the merits of Doe's Fifth Amendment claim. Part III upholds Doe's invocation of his Fifth Amendment right.

I.

This case began with the lawful seizure of seven pieces of digital media during the course of a child pornography investigation. In March 2010, law enforcement officials began an investigation of an individual using the YouTube.com account [redacted] whom the Government suspected of sharing explicit materials involving underage girls. During the course of their investigation, officers from the Santa Rosa County (Florida) Sheriff's office obtained several internet protocol ("IP") addresses from which [redacted] accessed the internet. Three of these IP addresses were then traced to hotels. Following a review of the hotels' guest registries, law enforcement officers found that the sole common hotel registrant during the relevant times was Doe.

In October 2010, law enforcement officers tracked Doe to a hotel in California and applied for a warrant to search his room. A judge granted the application and issued a search warrant, allowing the officers to seize all digital media, as well as any encryption devices or codes necessary to access such media. The officers seized seven pieces of digital media: two laptops—a 320–gigabyte ("GB") Dell Studio laptop and a 160–GB laptop; and five external hard drives—a 1.5–terabyte ("TB") Seagate external drive, a 1–TB Western Digital MyPassport external drive, a 1–TB external drive, a 500–GB Western Digital external drive, a 500–GB SimpleTech external drive. Federal Bureau of Investigation forensic examiners analyzed the digital media, but were unable to access certain portions of the hard drives.

The grand jury subpoena issued because the forensic examiners were unable to view the encrypted portions of the drives. The subpoena required Doe to produce the "unencrypted contents" of the digital media, and "any and all containers or folders thereon." Doe informed the U.S. Attorney that compliance with the subpoena would violate his Fifth Amendment privilege against self-incrimination. It was in an attempt to avoid this constitutional issue that the U.S. Attorney requested that the district court grant Doe the limited act-of-production immunity.

Thus, the focus of the motion to show cause hearing on April 19, 2011, was, in essence, whether the Fifth Amendment would bar the Government from establishing before a petit jury—say, if Doe were indicted for possession of child pornography in violation of 18 U.S.C. § 2252—that the decrypted contents (child pornography) were Doe's because (1) the hard drives belonged to Doe (which was not in dispute), and (2) contained child pornography. Doe contended that the establishment of point (2) would constitute the derivative use of his immunized grand jury testimony. That is, by decrypting the contents, he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the ***1340** contents, and could retrieve and examine them

whenever he wished.[9]

The critical testimony during the show cause hearing came from forensic examiner Timothy McCrohan. McCrohan testified that he cloned over 5 TB of data from the digital media devices—an "enormous amount of data." He also testified that over a million pieces of data could be stored on a typical 320–GB hard drive. McCrohan continued, "So when you're at five terabytes you're looking at 20 times that size. It could be in the multi-millions." Notably, McCrohan testified that the forensic examination indicated that the hard drives had been encrypted with a software program called "TrueCrypt." Essentially, TrueCrypt can make certain data inaccessible; in doing so, the program can create partitions within a hard drive so that even if one part of the hard drive is accessed, other parts of the hard drive remain secured. Because the hard drive was encrypted, the forensic examiners were unable to recover any data.[10] Although they were unable to find any files, McCrohan testified that they believed that data existed on the still-encrypted parts of the hard drive. In support of this belief, the Government introduced an exhibit with nonsensical characters and numbers, which it argued revealed the encrypted form of data that it seeks.

In his testimony on cross-examination by Doe, however, McCrohan conceded that, although encrypted, it was possible that the hard drives contain nothing. Doe asked McCrohan, "So if a forensic examiner were to look at an external hard drive and just see encryption, does the possibility exist that there actually is nothing on there other than encryption? In other words, if the volume was mounted, all you would see is blank. Does that possibility exist?" McCrohan responded: "Well, you would see random characters, but you wouldn't know necessarily whether it was blank."[11]

The forensic analysis was able to identify two passwords, neither of which revealed any information when entered. When pressed by Doe to explain why investigators believed something may be hidden, McCrohan replied, "The scope of my examination didn't go that far." In response to further prodding, "What makes you think that there are still portions that have data[?]," McCrohan responded, "We couldn't get into them, so we can't make that call." Finally, when asked whether "random data is just random data," McCrohan concluded that "anything is possible." At the conclusion of the hearing, the district court held Doe in contempt and committed him to the custody of the United States Marshal.[12]

*1341 II.

We turn now to the merits of Doe's appeal. In compelling Doe to produce the unencrypted contents of the hard drives and then in holding him in contempt for failing to do so, the district court concluded that the Government's use of the unencrypted contents in a prosecution against Doe would not constitute the derivative use of compelled testimony protected by the Fifth Amendment privilege against self-incrimination. This is

so, the court thought, because Doe's decryption and production of the hard drives would not constitute "testimony." And although that was the Government's view as well, the Government nonetheless requested act-of-production immunity.[13] The district court granted this request.

For the reasons that follow, we hold that Doe's decryption and production of the hard drives' contents would trigger Fifth Amendment protection because it would be testimonial, and that such protection would extend to the Government's use of the drives' contents. The district court therefore erred in two respects. First, it erred in concluding that Doe's act of decryption and production would not constitute testimony. Second, in granting Doe immunity, it erred in limiting his immunity . . . to the Government's use of his act of decryption and production, but allowing the Government derivative use of the evidence such act disclosed.

A.

"[I]n the context of a grand jury inquiry ... 'the public ... has a right to every man's evidence,' except for those persons protected by a constitutional, common-law, or statutory privilege." *United States v. Nixon,* 418 U.S. 683, 709, 94 S.Ct. 3090, 3108, 41 L.Ed.2d 1039 (1974) (quoting *United States v. Bryan,* 339 U.S. 323, 331, 70 S.Ct. 724, 730, 94 L.Ed. 884 (1949)). The Fifth Amendment provides, however, that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. Thus, the privilege against self-incrimination carves out a significant exception to the government's ability to obtain every man's evidence.

An individual must show three things to fall within the ambit of the Fifth Amendment: (1) compulsion, (2) a testimonial communication or act, and (3) incrimination. *See United States v. Ghidoni,* 732 F.2d 814, 816 (11th Cir.1984) (citing *United States v. Authement,* 607 F.2d 1129, 1131 (5th Cir.1979) (per curiam)). Here, the Government appears to concede, as it should, that the decryption and production are compelled and incriminatory. We need not pause any further, as it is obvious that the Government seeks, through the district court's order, to compel Doe to decrypt and hand over the contents of the drives, which, the Government argues, likely contain incriminatory evidence of ***1342** child pornography.[15]

The crux of the dispute here is whether the Government sought "testimony" within the meaning of the Fifth Amendment. The Government claims that it did not, that all it wanted Doe to do was merely to hand over pre-existing and voluntarily created files, not to testify. *See United States v. Hubbell,* 530 U.S. 27, 35–36, 120 S.Ct. 2037, 2043, 147 L.Ed.2d 24 (2000) (noting that it is a "settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege"). We agree—the files, if there are any at all in the hidden portions of the

hard drives, are not themselves testimonial.

Whether the drives' contents are testimonial, however, is not the issue. What is at issue is whether the *act of production* may have some testimonial quality sufficient to trigger Fifth Amendment protection when the production explicitly or implicitly conveys some statement of fact. *See Fisher v. United States,* 425 U.S. 391, 410, 96 S.Ct. 1569, 1581, 48 L.Ed.2d 39 (1976) ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced."). Thus, we focus on whether Doe's act of decryption and production would have been testimonial.

1.

Two seminal cases frame our analysis: *Fisher v. United States* and *United States v. Hubbell.* We start our discussion with this background.

In *Fisher,* the Court considered two Internal Revenue Service ("IRS") investigations, one in the Third Circuit and one in the Fifth Circuit, where the IRS sought to obtain voluntarily prepared documents the taxpayers had given to their attorneys. *Fisher,* 425 U.S. at 393–94, 96 S.Ct. at 1572. In each investigation, the IRS issued a summons requiring the taxpayer's attorney to hand over the documents, which included an accountant's work papers, copies of the taxpayer's returns, and copies of other reports and correspondence. *Id.* at 394, 96 S.Ct. at 1572–73. When the attorney refused to comply with the summons on the ground that the documents were privileged and, moreover, protected by his Fifth Amendment privilege against self-incrimination, the IRS brought an enforcement action in district court. * * * In both cases, the district court granted relief, ordering the attorney to comply with the summons, and its decision was appealed. *Id.*

After granting certiorari, the Supreme Court made short shrift of the attorneys' argument that the Fifth Amendment protected them from producing the documents in their possession, holding that they could not invoke the privilege. 425 U.S. at 397–402, 96 S.Ct. at 1574–76. Turning to the taxpayers' privilege, the Court treated the taxpayers as retaining possession of the documents [because of attorney-client confidentiality]. *Id.* at 405, 96 S.Ct. at 1578. It then held that the taxpayers' act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate them. *Id.* at 410, 96 S.Ct. at 1581. In the cases before it, though, the Court concluded that the act of producing the subpoenaed documents would not involve testimonial self-incrimination because the Government was in "no way relying on the truth telling of the taxpayer." *Id.* at 411, 96 S.Ct. at 1581 (internal quotation marks omitted). This explanation became known as the "foregone conclusion" doctrine. The Court expressed it thusly:

> It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment.... Surely the Government is in no way relying on the "truth telling" of the taxpayer to prove the existence of or his access to the documents. The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender."
> *Id.* (quoting *In re Harris,* 221 U.S. 274, 279, 31 S.Ct. 557, 558, 55 L.Ed. 732 (1911) (citation omitted)).[19]

***1344** The Court reasoned that, in essence, the taxpayers' production of the subpoenaed documents would not be testimonial because the Government knew of the existence of the documents, knew that the taxpayers possessed the documents, and could show their authenticity not through the use of the taxpayers' mind, but rather through testimony from others. *Id.* Where the location, existence, and authenticity of the purported evidence is known with reasonable particularity,[20] the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available.

Twenty-four years after *Fisher,* the Court decided *Hubbell.* In *Hubbell,* a grand jury investigating the activities of Whitewater Development Corporation issued a subpoena duces tecum requiring Hubbell to provide eleven categories of documents. 530 U.S. at 30–31, 120 S.Ct. at 2040. Hubbell invoked the Fifth Amendment privilege, so the Government obtained a district court order granting Hubbell § 6002 immunity. *Id.* at 31, 120 S.Ct. at 2040. Hubbell complied with the subpoena and turned over 13,120 pages of documents. *Id.*

The grand jury subsequently returned a ten-count indictment charging Hubbell with several federal crimes. *Id.* at 31, 120 S.Ct. at 2041. Asserting that the Government could not convict him without the immunized documents, Hubbell moved the district court to dismiss the indictment. *Id.* at 31–33, 120 S.Ct. at 2041. The court held a hearing, found that the Government could not show that it had knowledge of the contents of the documents from a source independent of the documents themselves, and dismissed the indictment. The Government appealed the dismissal. *Id.* at 31–32, 120 S.Ct. at 2041.[21]

The Supreme Court granted a writ of certiorari. *Id.* at 34, 120 S.Ct. at 2042. The Court held that Hubbell's act of production was sufficiently testimonial to trigger Fifth Amendment protection, as knowledge of the implicit testimonial facts associated with his act of production was not a foregone conclusion. *Id.* at 44–45, 120 S.Ct. at 2047–48. In so holding, the Court distinguished *Fisher:*

> Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it. While in ***1345** *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. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.

Id. at 44–45, 120 S.Ct. at 2048. In *Fisher,* therefore, the act of production was not testimonial because the Government had knowledge of each fact that had the potential of being testimonial. As a contrast, the Court in *Hubbell* found there was testimony in the production of the documents since the Government had no knowledge of the existence of documents, other than a suspicion that documents likely existed and, if they did exist, that they would fall within the broad categories requested.[22] *See id.* at 44–45, 120 S.Ct. at 2047–48.

Drawing out the key principles from the Court's two decisions, an act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic. *See id.* at 36 & n. 19, 120 S.Ct. at 2043 & n. 19. The touchstone of whether an act of production is testimonial is whether the government compels the individual to use "the contents of his own mind" to explicitly or implicitly communicate some statement of fact. *Curcio v. United States,* 354 U.S. 118, 128, 77 S.Ct. 1145, 1151, 1 L.Ed.2d 1225 (1957).

Put another way, the Court has marked out two ways in which an act of production is *not testimonial.* First, the Fifth Amendment privilege is not triggered where the Government merely compels some physical act, i.e. where the individual is not called upon to make use of the contents of his or her mind. The most famous example is the key to the lock of a strongbox containing documents, *see Hubbell,* 530 U.S. at 43, 120 S.Ct. at 2047 (citing *Doe v. United States,* 487 U.S. 201, 210 n. 9, 108 S.Ct. 2341, 2347 n. 9, 101 L.Ed.2d 184 (1988)), but the Court has also used this rationale in a variety of other contexts.[24] Second, under the "foregone ***1346** conclusion" doctrine, an act of production is not testimonial—even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed materials—if the Government can show with "reasonable particularity" that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a "foregone conclusion."

2.

With this framework in hand, we turn to the facts of this case. We hold that the act of

Doe's decryption and production of the contents of the hard drives would sufficiently implicate the Fifth Amendment privilege. We reach this holding by concluding that (1) Doe's decryption and production of the contents of the drives would be testimonial, not merely a physical act; and (2) the explicit and implicit factual communications associated with the decryption and production are not foregone conclusions.

First, the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature. We conclude that the decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files.

We are unpersuaded by the Government's derivation of the key/combination analogy in arguing that Doe's production of the unencrypted files would be nothing more than a physical nontestimonial transfer. The Government attempts to avoid the analogy by arguing that it does not seek the combination or the key, but rather the contents. This argument badly misses the mark. In *Fisher,* where the analogy was born, and again in *Hubbell,* the Government never sought the "key" or the "combination" to the safe for its own sake; rather, the Government sought the files being withheld, just as the Government does here. *Hubbell,* 530 U.S. at 38, 120 S.Ct. at 2044 (trying to compel production of documents); *Fisher v. United States,* 425 U.S. at 394–95, 96 S.Ct. at 1572–73 (seeking to access contents possessed by attorneys). Requiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by the implied factual statements noted above that could prove to be incriminatory. *See Hubbell,* 530 U.S. at 43, 120 S.Ct. at 2047. Hence, we conclude that what the Government seeks to compel in this case, the decryption and production of the contents of the hard drives, is testimonial in character.

Moving to the second point, the question becomes whether the purported testimony is a "foregone conclusion." We think not. Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives.

To support its position, the Government points to McCrohan's testimony. It states in its answer brief that "[h]ere, the government knows of the 'existence' and 'whereabouts' of the decrypted records it has subpoenaed because the government *already* ***1347** *physically* possesses those records." Answer Br. at 22. But McCrohan's testimony simply does not stretch as far as the Government wishes it would. As an initial matter, McCrohan admitted on cross-examination that he had no idea whether there was data on the encrypted drives. Responding to a question from Doe as to whether the random

characters definitively indicated that encrypted data is present or instead could have indicated blank space, McCrohan conceded, "Well, you would see random characters, but you wouldn't know necessarily whether it was blank." Moreover, when pressed to answer why investigators believed data may be hidden, McCrohan replied, "The scope of my examination didn't go that far," and, "We couldn't get into them, so we can't make that call." Finally, when Doe posed the question of whether "random data is just random data," McCrohan concluded that "anything is possible."

To be fair, the Government has shown that the combined storage space of the drives *could* contain files that number well into the millions. And the Government has also shown that the drives are encrypted. The Government has not shown, however, that the drives *actually* contain any files, nor has it shown which of the estimated twenty million files the drives are capable of holding may prove useful. The Government has emphasized at every stage of the proceedings in this case that the forensic analysis showed random characters. But random characters are not files; because the TrueCrypt program displays random characters if there are files *and* if there is empty space, we simply do not know what, if anything, was hidden based on the facts before us. It is not enough for the Government to argue that the encrypted drives are *capable* of storing vast amounts of data, some of which *may* be incriminating. In short, the Government physically possesses the media devices, but it does not know what, if anything, is held on the encrypted drives.[25] Along the same lines, we are not persuaded by the suggestion that simply because the devices were encrypted necessarily means that Doe was trying to hide something. Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all.

In sum, we think this case is far closer to the *Hubbell* end of the spectrum than it is to the *Fisher* end. As in *Hubbell,* "the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the [files]" that it seeks to compel Doe to produce. *Hubbell,* 530 U.S. at 45, 120 S.Ct. at 2048. In *Fisher,* the Government knew exactly what documents it sought to be produced, knew that they were in the possession of the attorney, and knew that they were prepared by an accountant. 425 U.S. at 411–12, 96 S.Ct. at 1581. Here, the Government has not shown that it possessed even a remotely similar level of knowledge as to the *files* on the hard drives at the time it attempted to compel production from Doe. Case law from the Supreme Court does not demand that the Government identify exactly the documents it seeks, but it does require some specificity in its requests—categorical requests for documents the Government anticipates are likely to exist simply will not suffice. *See Hubbell,* 530 U.S. at 45, 120 S.Ct. at 2048 ("The Government cannot cure this [lack of prior knowledge] through the over broad argument that a ***1348** businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena."); *Doe,* 465 U.S. at 613–14 & nn. 11–13, 104 S.Ct. at 1242–43 & nn. 11–13 (holding that the act of producing vast categories of records was privileged under the Fifth Amendment and could not be compelled absent a grant of immunity).

The Government tries to analogize this case to *In re Boucher,* No. 2:06–mj–91, 2009 WL 424718 (D.Vt. Feb. 19, 2009). The facts of *Boucher* appear to be somewhat similar to the facts of this case, but we do not find the Government's analogy persuasive.[26] Like this case, in *Boucher* the Government sought to compel a suspect to produce an unencrypted version of a drive on his laptop. *Id.* at *1. Previously, the Government had reviewed portions of the encrypted drive with the suspect but was unable to reopen the drive once it was closed. *Id.* at *1–2. During this initial viewing, law enforcement officers examined the encrypted and unencrypted portions of the suspect's hard drive. *Id.* at *2. After observing images of animated child pornography on the unencrypted portions of the hard drive, a Special Agent from Immigration and Customs Enforcement ("ICE") with experience and special training in recognizing child pornography was called. *Id.* The ICE agent examined the computer and saw a file labeled "2yo getting raped during diaper change," but was unable to open it. *Id.* After the suspect navigated to the encrypted portion of the hard drive, the ICE agent located and examined several videos or images that appeared to be child pornography. *Id.* The district court concluded that the "foregone conclusion" doctrine applied under those facts because any testimonial value derived from the act of production was already known to the Government and therefore added nothing to its case. *Id.* at *3–4.

The Government correctly notes that *Boucher* did not turn on the fact that the Government knew the contents of the file it sought, *id.* at *3; *Fisher* and *Hubbell,* though, still require that the Government show its knowledge *that the files exist.* Thus, while in *Boucher* it was irrelevant that the Government knew what was contained in the file "2yo getting raped during diaper change," it was crucial that ***1349** the Government knew that there existed a file under such a name.[27] *Id.* That is simply not the case here. We find no support in the record for the conclusion that the Government, at the time it sought to compel production, knew to any degree of particularity what, if anything, was hidden behind the encrypted wall.[28]

In short, we conclude that Doe would certainly use the contents of his mind to incriminate himself or lead the Government to evidence that would incriminate him if he complied with the district court's order. Moreover, the Government has failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that Doe has access to those files, or that he is capable of decrypting the files. The "foregone conclusion" doctrine does not apply under these facts.

The Fifth Amendment protects Doe's refusal to decrypt and produce the contents of the media devices because the act of decryption and production would be testimonial, and because the Government cannot show that the "foregone conclusion" doctrine applies.

B.

The district court still could have compelled Doe to turn over the unencrypted contents—and held him in contempt if he refused to do so—had the Government offered and the district court granted Doe ***1350** constitutionally sufficient immunity. The district court erred in limiting Doe's immunity under 18 U.S.C. §§ 6002 and 6003 to the Government's use of his act of decryption and production while allowing the Government derivative use of the evidence such act disclosed. Doe's immunity was not coextensive with the protections afforded by the Fifth Amendment; consequently, he could not have been compelled to decrypt and produce the contents of the hard drives.

In evaluating the immunity Doe received, we must look beyond the act-of-production label and ask this question: what conduct was actually immunized and what use would the Government make of the evidence derived from such conduct in a future prosecution? * * *

In the seminal case on point, *Kastigar v. United States,* the Court stated:

> The constitutional inquiry, rooted in logic and history, as well as in the decisions of this Court, is whether the immunity granted under this statute is coextensive with the scope of the privilege. If so, petitioners' refusals to answer based on ***1351** the privilege were unjustified, and the judgments of contempt were proper, for the grant of immunity has removed the dangers against which the privilege protects. If, on the other hand, the immunity granted is not as comprehensive as the protection afforded by the privilege, petitioners were justified in refusing to answer, and the judgments of contempt must be vacated.

Kastigar v. United States, 406 U.S. 441, 449, 92 S.Ct. 1653, 1659, 32 L.Ed.2d 212 (1972) (footnote and citation omitted) (citing *McCarthy v. Arndstein,* 266 U.S. 34, 42, 45 S.Ct. 16, 17, 69 L.Ed. 158 (1924)). The Court then held that § 6002 "immunity from use and derivative use is coextensive with the scope of the [Fifth Amendment] privilege against self-incrimination." *Id.* at 453, 92 S.Ct. at 1661. In so holding, the Court emphasized that such immunity "prohibits the prosecutorial authorities from using the compelled testimony in any respect." *Id.*

Supreme Court precedent is clear: Use and derivative-use immunity establishes the critical threshold to overcome an individual's invocation of the Fifth Amendment privilege against self-incrimination. No more protection is necessary; no less protection is sufficient.[32] * * *

The Government gave no such immunity in this case. In essence, the Government attempted to immunize the testimony itself, treating everything else as fair game. But for the reasons we just noted, the Government cannot obtain immunity only for the act of production and then seek to introduce the contents of the production, regardless of

whether those contents are characterized as nontestimonial evidence, because doing so would allow the use of evidence *derived* from the original testimonial ***1352** statement.[33]

The Court in *Hubbell* expressly rejected the "manna from heaven" theory, which contended that if the Government omitted any description of how the documents were obtained, it would be as if they magically appeared on the courthouse steps and the Government could use the documents themselves.[34] 530 U.S. at 33, 42, 120 S.Ct. at 2041–42, 2046–47. The Government, in essence, asks us to revisit the "manna from heaven" theory. The Supreme Court definitively foreclosed such an argument; hence, we must decline to consider it.

To conclude, because Doe's act of production would have testimonial aspects to it, an order to compel him to produce the unencrypted contents of the drives would require immunity coextensive with the Fifth Amendment (and § 6002). Immunity coextensive with the Fifth Amendment requires both use and derivative-use immunity. The Government's offer of act-of-production immunity clearly could not provide the requisite protection because it would allow the Government to use evidence derived from the immunized testimony. Thus, because the immunity offered here was not coextensive with the Fifth Amendment, Doe could not be compelled to decrypt the drives.

III.

We hold that Doe properly invoked the Fifth Amendment privilege. In response, the Government chose not give him the immunity the Fifth Amendment and ***1353** 18 U.S.C. § 6002 mandate, and the district court acquiesced. Stripped of Fifth Amendment protection, Doe refused to produce the unencrypted contents of the hard drives. The refusal was justified, and the district court erred in adjudging him in civil contempt. The district court's judgment is accordingly REVERSED.

SO ORDERED.

Footnotes

[1] The contents of the drives were encrypted. The subpoena required Doe to decrypt and produce the contents.

[5] Doe appeared without counsel at this hearing and the show cause hearing held later that day.

[6] As indicated *supra* note 5, Doe appeared before the court without counsel. Our statement of Doe's explanation for invoking the Fifth Amendment expresses the gist of Doe's position, not the precise words he used.

[9] At the show cause hearing, there was no evidence that Doe was the only person who had access to his hard drives. Nor was there any evidence that he was capable of decrypting the drives' contents.

[10] McCrohan stated that he accessed parts of the drive only to find "a blank area of the hard drive, and there was no data, you know, physically, that we were able to see."

[11] McCrohan's admission that blank space appears as random characters is supported by TrueCrypt's description on its website: "[F]ree space on any TrueCrypt volume is always filled with random data when the volume is created and no part of the (dismounted) hidden volume can be distinguished from random data." *Hidden Volume,* TrueCrypt, http://www.truecrypt.org/docs/?s =hidden-volume (last visited January 31, 2012).

[12] The district court announced its decision from the bench and later the same day memorialized it in a written order. The order adjudged Doe guilty of criminal contempt. A revised order issued two days later stated that Doe had been adjudged in civil contempt. On April 21, 2011, Doe again appeared before the grand jury. He refused to produce the unencrypted contents of the hard drives and therefore remained incarcerated in the Marshal's custody. On December 15, 2011, after hearing oral argument in Doe's appeal, we ordered Doe released from custody.

[13] If the decryption of the hard drives would not constitute testimony, one must ask, "Why did the Government seek, and the district court grant, immunity for Doe's decryption?" The answer is obvious: Doe's decryption would be testimonial.

[15] As we explain in greater detail in part II.B *infra,* even if the decryption and production of the contents of the hard drives themselves are not incriminatory, they are a "link in the chain of evidence" that is designed to lead to incriminating evidence; this is sufficient to invoke the Fifth Amendment privilege. *Hoffman v. United States,* 341 U.S. 479, 486, 71 S.Ct. 814, 818, 95 L.Ed. 1118 (1951) ("The privilege afforded [by the Fifth Amendment] not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."); *see also United States v. Hubbell,* 530 U.S. 27, 38, 120 S.Ct. 2037, 2044, 147 L.Ed.2d 24 (2000) ("Compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory." (quoting *Doe v. United States,* 487 U.S. 201, 208 n. 6, 108 S.Ct. 2341, 2346 n. 6, 101 L.Ed.2d 184 (1988))); *Kastigar v. United States,* 406 U.S. 441, 444–45, 92 S.Ct. 1653, 1656, 32 L.Ed.2d 212 (1972) ("[The Fifth Amendment privilege] can be asserted in any proceeding, civil or criminal, administrative or judicial, investigatory or adjudicatory; and it protects against any disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used." (footnote omitted)).

[19] The "foregone conclusion" doctrine is a method by which the Government can show that no testimony is at issue. This is related to, but distinct from, the Government's task in a criminal case brought against an individual given use and derivative-use immunity to show that evidence protected by the Fifth Amendment privilege is admissible because the Government could have obtained it from a "legitimate source, wholly independent of the compelled testimony." *Kastigar,* 406 U.S. at 460, 92 S.Ct. at 1665. If in the case at hand, for example, the Government could prove that it had knowledge of the files encrypted on Doe's hard drives, that Doe possessed the files, and that they were authentic, it could compel Doe to produce the contents of the files even though it had no independent source from which it could obtain the files.

[20] Both the Ninth and D.C. Circuits have adopted this "reasonable particularity" standard with regard to the "foregone conclusion" doctrine. *See United States v. Ponds,* 454 F.3d 313, 320–21 (D.C.Cir.2006); *In re Grand Jury Subpoena, Dated April 18, 2003,* 383 F.3d 905, 910 (9th Cir.2004). We are persuaded by their reasoning and now follow suit.

[21] The court of appeals vacated the dismissal and remanded the case with the instruction that the district court determine whether the Government could show knowledge of the existence and authenticity of the documents and the defendant's possession or control of them, not whether it knew of the contents of the documents. *Hubbell,* 530 U.S. at 33–34, 120 S.Ct. at 2041. On remand, the Government conceded that it could not prove the requisite level of knowledge and, instead, entered into a plea agreement that provided for the dismissal of the charges against Hubbell unless the Supreme Court, granting the Government's petition for a writ of certiorari, ruled that his act of production was not "a significant bar" to the prosecution. *Id.* at 33, 120 S.Ct. at 2042.

[22] The Court then held that, in light of the grant of immunity for the testimonial act of production, the Government could not introduce the contents of the documents in a later prosecution without showing "that the evidence it used in obtaining the indictment and proposed to use at trial was derived from legitimate sources 'wholly independent' of the testimonial aspect of respondent's immunized conduct in assembling and producing the documents described in the subpoena." *Hubbell,* 530 U.S. at 45, 120 S.Ct. at 2048. Because the Government could not make that showing, the use of the documents derived directly or indirectly from the testimonial act of production violated the respondent's Fifth Amendment privilege. *Id.* This aspect of the holding is relevant to part II.B, discussed *infra.*

[24] *See e.g., United States v. Dionisio,* 410 U.S. 1, 7, 93 S.Ct. 764, 768, 35 L.Ed.2d 67 (1973) (holding that providing a voice exemplar is not testimonial); *Gilbert v. California,* 388 U.S. 263, 266, 87 S.Ct. 1951, 1953, 18 L.Ed.2d 1178 (1967) (concluding that providing a handwriting exemplar is not testimonial); *United States v. Wade,* 388 U.S. 218, 222–23, 87 S.Ct. 1926, 1930, 18 L.Ed.2d 1149 (1967) (holding that standing in a lineup is not

testimonial); *Schmerber v. California,* 384 U.S. 757, 765, 86 S.Ct. 1826, 1833, 16 L.Ed.2d 908 (1966) (concluding that furnishing a blood sample is not testimonial); *Holt v. United States,* 218 U.S. 245, 252–53, 31 S.Ct. 2, 6, 54 L.Ed. 1021 (1910) (determining that wearing particular clothing is not testimonial).

[25] This situation is no different than if the Government seized a locked strongbox. Physical possession of the entire lockbox is not the issue; whether the Government has the requisite knowledge of what is contained inside the strongbox is the critical question.

[26] In *Boucher,* border protection officers inspected a car as it crossed the border from Canada. *In re Boucher,* No. 2:06–mj–91, 2009 WL 424718, *1–2 (D.Vt. Feb. 19, 2009). After directing the car into a "secondary inspection," an officer found a laptop computer in the backseat, which he was able to search access without a password. *Id.* at *1. The officer located 40,000 images, some of which appeared to be child pornography based on their file names. *Id.* at *1–2. A special agent from Immigration and Customs Enforcement ("ICE") was called to continue the investigation. *Id.* at *2. The ICE agent was unable to open certain files to view the contents, but was able to determine that they had been opened at some point previously. *Id.* The ICE agent then read Boucher his Miranda rights and began questioning him about child pornography files the agent thought might be on the computer. *Id.* Boucher admitted he sometimes inadvertently downloaded images of child pornography. At the officer's request, Boucher navigated to the encrypted portion of the laptop's hard drive, i.e., the "Z" drive, which the officer searched and viewed several images of suspected child pornography. Boucher was then arrested. *Id.* A forensic examination was made of the computer's drives. *Id.* The contents of all but one drive were revealed. *Id.* The contents of the "Z" drive had been encrypted. *Id.* To gain access to the encrypted drive, the Government had a grand jury issue a subpoena directing Boucher to provide the unencrypted contents of the drive. *Id.* Boucher moved to quash, asserting his Fifth Amendment privilege. *Id.*

[27] It is because of the Government's lack of knowledge in this case that we can easily distinguish another recent decision, *United States v. Fricosu,* No. 10–cr–00509–REB–02, —— F.Supp.2d ——, 2012 WL 182121 (D.Colo. Jan. 23, 2012). In *Fricosu,* the Government, after seizing a laptop computer suspected of containing incriminating information, was unable to access certain encrypted portions of the computer. *Id.* at ——, 2012 WL 182121 at *2. The Government sought a court order requiring Fricosu to produce the unencrypted contents of the computer, and Fricosu invoked her Fifth Amendment privilege against self-incrimination. *Id.* The court then concluded that no testimony was associated with the compelled production of the unencrypted contents of her laptop computer. *Id.* at ——, 2012 WL 182121 at *4. In reaching this conclusion, the court heavily relied upon a tape recording of a phone call introduced by the Government between Fricosu and another individual, where the defendant admitted, "[The content at issue] was on my laptop." *Id.* at ——, 2012 WL 182121 at *2. Fricosu later confirmed in the call that the content existed when she was asked, "It was on your laptop[?]," and

Fricosu responded, "Yes." *Id.* Throughout this extensive exchange, Fricosu essentially admitted every testimonial communication that may have been implicit in the production of the unencrypted contents. Here, in contrast, the Government does not know whether any files are present on the encrypted drive; whether Doe has access to and control over the encrypted drives; and whether Doe is capable of decryption.

28 To be clear, the Government does not have to show that it knows specific file names. Knowledge of a file name, like the Government had in *Boucher,* would be an easy way for the Government to carry its burden of showing that the existence of the files it seeks is a "foregone conclusion." That said, if 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. *See United States v. Norwood,* 420 F.3d 888, 895–96 (8th Cir.2005) (applying "foregone conclusion" doctrine even though the Government could not identify a specific bank account because the Government was able to prove the name and location of the entity that created the records, introduced payment card numbers, and produced the details of transactions involving the account). 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. Here, the Government was unable to do that.

30 The Government's decision to offer only act-of-production immunity was done with an eye for the future. The act of decrypting the hard drives would not be introduced as evidence against Doe in a criminal prosecution. But, given the district court's decision, the derived evidence would be introduced unless this court reversed in this appeal the district court's order. If we upheld the order and Doe moved the court in a subsequent criminal prosecution to bar the evidence as obtained in violation of the Fifth Amendment, the Government would no doubt contend that our decision had settled the issue.

32 The *Kastigar* Court concluded that transactional immunity—a prohibition on any future prosecution based on immunized testimony—exceeded the protections offered by the Fifth Amendment, but that immunity limited to the prohibition on the use of the testimonial evidence itself, not derivative evidence, offered too little protection to compel production:

> We hold that such immunity from use and derivative use is coextensive with the scope of the privilege against self-incrimination, and therefore is sufficient to compel testimony over a claim of the privilege. While a grant of immunity must afford protection commensurate with that afforded by the privilege, it need not be broader. Transactional immunity, which accords full immunity from prosecution for the offense to which the compelled testimony relates, affords the witness considerably broader protection than does the Fifth Amendment privilege. The privilege has never been construed to mean that one who invokes it cannot subsequently be prosecuted. Its sole concern is to afford protection against being "forced to give testimony leading to the infliction of 'penalties affixed to ... criminal acts.' " Immunity from the use of

compelled testimony, as well as evidence derived directly and indirectly therefrom, affords this protection.

Kastigar, 406 U.S. at 453, 92 S.Ct. at 1661 (footnote omitted) (quoting *Ullmann v. United States,* 350 U.S. 422, 438–39, 76 S.Ct. 497, 507, 100 L.Ed. 511 (1956)).

[33] The D.C. Circuit, addressing a similar issue, reached the same conclusion. *See Ponds,* 454 F.3d at 328 ("[N]on-testimonial evidence derived from this testimonial act of production may not be used under § 6002."). That court provided a useful analogy to clarify how act-of-production immunity can be problematic:

> [I]f a murder suspect who has been granted immunity is called before a grand jury and asked whether he committed a murder and where the murder weapon is, his testimony may not be used against him in a criminal trial. In addition, the government may not use his testimony to retrieve the weapon for use against the witness at trial. Even if the government introduced the weapon without indicating that it learned of its location from the defendant's immunized grand jury testimony, only using fingerprints or DNA testing to link the weapon to the defendant, the weapon would still be barred because it was "directly or indirectly derived from" compelled testimony. If the police simply happened upon the weapon through an ongoing investigation, however, the weapon could be used against the witness because it was "derived from a legitimate source wholly independent of the compelled testimony."

Id. at 321 (quoting *Kastigar,* 406 U.S. at 460, 92 S.Ct. at 1665). We think this is analogous to the case here. Essentially the Government asks that we compel Doe to provide incriminating testimony—producing the unencrypted documents. The Government then argues that it will not use the compelled testimony. The problem, though, is that the contents of the drives would still be barred because they would be "directly or indirectly derived from" compelled testimony. *Kastigar,* 406 U.S. at 453, 92 S.Ct. at 1661 (internal quotation marks omitted). Thus, because the protection offered by the act-of-production immunity is not coextensive with the Fifth Amendment, Doe was within his right to refuse to decrypt the drives and the court cannot compel him to do otherwise.

[34] The Court stated:

> It is abundantly clear that the testimonial aspect of respondent's act of producing subpoenaed documents was the first step in a chain of evidence that led to this prosecution. The documents did not magically appear in the prosecutor's office like "manna from heaven." They arrived there only after respondent asserted his constitutional privilege, received a grant of immunity, and—under the compulsion of the District Court's order—took the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena.

Hubbell, 530 U.S. at 42, 120 S.Ct. at 2046–47.