SJC-11358

COMMONWEALTH vs. LEON I. GELFGATT.

Suffolk. November 5, 2013. - June 25, 2014.

Present: Ireland, C.J., Spina, Cordy, Botsford, Gants, Duffly, & Lenk, JJ.

Forgery. Uttering Forged Instrument. Larceny. False Pretenses. Witness, Compelling giving of evidence, Self-incrimination. Evidence, Information stored on computer, Testimonial statement. Search and Seizure, Computer. Constitutional Law, Self-incrimination.

Indictments found and returned in the Superior Court Department on May 7, 2010.

A pretrial motion to compel evidence was heard by Raymond J. Brassard, J., and a question of law was reported by him.

The Supreme Judicial Court on its own initiative transferred the case from the Appeals Court.

Randall E. Ravitz, Assistant Attorney General (Thomas D. Ralph, Assistant Attorney General, with him) for the Commonwealth.

Paul Joseph Davenport (Stanley D. Helinski with him) for the defendant.

The following submitted briefs for amici curiae:

Daniel B. Garrie, of Washington, & Daniel K. Gelb, for Daniel K. Gelb & others.

David H. Margolis, of Florida, for Florida Department of Law Enforcement & others.

Mark R. Gage & Christian J. Desilets, of West Virginia, for

National White Collar Crime Center.

David W. Opderbeck, of New Jersey, for David W. Opderbeck & others.

Nathan F. Wessler, of New York, Hanni M. Fakhoury, of California, & Matthew R. Segal, Jessie J. Rossman, & Kit Walsh, for American Civil Liberties Union Foundation of Massachusetts & others.

Victoria L. Nadel, for Massachusetts Association of Criminal Defense Lawyers.

SPINA, J. On May 5, 2010, a State grand jury returned indictments charging the defendant with seventeen counts of forgery of a document, G. L. c. 267, § 1; seventeen counts of uttering a forged instrument, G. L. c. 267, § 5; and three counts of attempting to commit the crime of larceny by false pretenses of the property of another, G. L. c. 274, § 6. The charges arose from allegations that the defendant, through his use of computers, conducted a sophisticated scheme of diverting to himself funds that were intended to be used to pay off large mortgage loans on residential properties. On November 21, 2011, the Commonwealth filed in the Superior Court a "Motion to Compel the Defendant to Enter His Password into Encryption Software He Placed on Various Digital Media Storage Devices that Are Now in the Custody of the Commonwealth" (motion to compel decryption). The Commonwealth also filed a motion to report a question of law to the Appeals Court prior to trial pursuant to Mass. R. Crim. P. 34, as amended, 442 Mass. 1501 (2004). The question concerned the lawfulness of compelling the defendant to privately enter an encryption key into computers seized from him by the Commonwealth.[1] Following a hearing on January 18, 2012, a judge

[1] The parties treat as synonymous the terms "encryption key" and "password" to encryption software. For the sake of

denied the Commonwealth's motion to compel decryption, but he reported the following question of law:

> "Can the defendant be compelled pursuant to the Commonwealth's proposed protocol to provide his key to seized encrypted digital evidence despite the rights and protections provided by the Fifth Amendment to the United States Constitution and Article Twelve of the Massachusetts Declaration of Rights?"[2]

We transferred the case to this court on our own motion.[3] We now conclude that the answer to the reported question is, "Yes, where the defendant's compelled decryption would not communicate facts of a testimonial nature to the Commonwealth beyond what the defendant already had admitted to investigators." Accordingly, we reverse the judge's denial of the Commonwealth's motion to compel decryption.[4]

---

simplicity, we shall do the same.

[2] The parties have not included in the record appendix a copy of the order reporting the question of law from the Superior Court. We rely on a joint stipulation of the parties filed on July 19, 2012, that sets forth the language of the reported question.

[3] All proceedings in the Superior Court have been stayed pending resolution of the reported question.

[4] We acknowledge the amicus briefs submitted in support of the defendant by the American Civil Liberties Union Foundation of Massachusetts, the American Civil Liberties Union Foundation, and the Electronic Frontier Foundation; by the Massachusetts Association of Criminal Defense Lawyers; and by Daniel K. Gelb, Daniel B. Garrie, and the National Association of Criminal Defense Lawyers. We also acknowledge the amicus briefs submitted in support of the Commonwealth by David W. Opderbeck, the Massachusetts Chiefs of Police Association, Inc., and NW3C, Inc., doing business as the National White Collar Crime Center; by the Florida Department of Law Enforcement, the Massachusetts Chiefs of Police Association, Inc., NW3C, Inc., doing business as the National White Collar Crime Center, and the National District Attorneys Association; and by NW3C, Inc., doing business as the National White Collar Crime Center.

1. Background. The undisputed facts are taken from the parties' submissions to the motion judge.[5]

Beginning in 2009, the defendant, who is an attorney, allegedly orchestrated a scheme to acquire for himself funds that were intended to be used to pay off home mortgage loans. According to the Commonwealth, the defendant identified high-end properties that were listed in an online database as "under agreement." He would research each one at the applicable registry of deeds to determine whether there was a mortgage on the property. If there was, the defendant, purportedly using a computer, would forge an assignment of the mortgage to either "Puren Ventures, Inc." (Puren Ventures) or "Baylor Holdings, Ltd." (Baylor Holdings). He then would record the forged assignment at the applicable registry of deeds and mail a notice to the seller stating that the mortgage on the property had been assigned to one of these sham companies, which he had set up.

The defendant fostered the illusion that Puren Ventures and Baylor Holdings were actual companies by giving each one

---

[5] These submissions included an affidavit dated August 31, 2011, from David Papargiris, the director of the Attorney General's computer forensics laboratory; an affidavit dated October 19, 2011, from State police Trooper Patrick M. Johnson; and the transcript of an audio recording of a postarrest interview of the defendant conducted on December 17, 2009, by law enforcement officers. The motion judge declined to make findings of fact when ruling on the Commonwealth's motion to compel decryption, given that the only facts before him were those presented in the Commonwealth's submissions. Defense counsel did not dispute the facts set forth in the affidavits and transcript, recognizing that they spoke for themselves. He did, however, point out that he might disagree with some of the characterizations of those facts.

Internet-based telephone and facsimile numbers. When a closing attorney would contact one of these companies to request a statement documenting the sum necessary to pay off the reassigned mortgage, the attorney would be instructed to send the request to the facsimile number that the defendant had created. Next, the defendant would request an actual payoff figure from the true mortgage holder. The defendant would transmit this information by Internet facsimile number to the closing attorney, doing so under the guise of the sham company. The defendant would instruct the closing attorney to send the payoff check to a Boston address where the defendant once had practiced law. Although ultimately unsuccessful, the defendant purportedly created seventeen fraudulent assignments of mortgages, totaling over $13 million. According to the Commonwealth, the defendant relied heavily on the use of computers to conceal his identity and perpetrate his alleged scheme.

On December 17, 2009, State police troopers arrested the defendant immediately after he retrieved what he believed to be over $1.3 million in payoff funds from two real estate closings. They also executed search warrants for his residence in Marblehead and for his vehicle. During the search of the defendant's residence, troopers observed several computers that were powered on, and they photographed the computer screens.[6]

[6] Appearing on the computer screens were the following phrases that were visible as headings or icons: "K:\Leon Documents\My Scans"; "Erasing Report"; "Erased area"; "Attorney Leon I. Gelfgatt"; "TrueCrypt"; and "DriveCrypt Plus Pack."

The troopers seized from the defendant's residence two desktop computers, one laptop computer, and various other devices capable of storing electronic data.[7] They also seized one smaller "netbook" computer from the defendant's vehicle. Computer forensic examiners were able to view several documents and "bookmarks" to Web sites that were located on an external hard drive.[8] However, all of the data on the four computers were encrypted with "DriveCrypt Plus" software.[9]

---

[7] Apart from the computers, troopers seized an Adaptec external hard drive, two universal serial bus (USB) thumb drives, two secure digital cards, two cellular telephones, and fourteen compact discs.

[8] These documents included what appeared to be unsigned releases for a mortgage encumbering the defendant's residential property in Marblehead. Computer forensic examiners also were able to see an image file that appeared to contain the seal for an Arizona notary public. The "bookmarks" included a Web site where Puren Ventures was advertised for sale, and a Web site offering anonymous wire transfers.

[9] In an affidavit submitted in connection with the Commonwealth's motion to compel decryption, the director of the Attorney General's computer forensics laboratory explained the differences between encryption and decryption:

> "Encryption is the process by which 'readable' digital media, that is, digital media or data that can be viewed and accessed, is scrambled in such a way as to render that digital media or data 'unreadable' without decryption. Encryption can be performed both by hardware and by means of software tools.
>
> "Decryption is the process by which encrypted, scrambled data is rendered 'readable' again. In order to decrypt data, the person seeking decryption performs some action such as the entering of a password, scanning of a fingerprint or [insertion of] a USB Thumb drive with a pass code key on it. The encryption software then translates this action into a 'key,' essentially a string of numbers or characters. The encryption software then applies this key to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through

According to the Commonwealth, the encryption software on the computers is virtually impossible to circumvent. Its manufacturer touts the fact that it does not contain a "back door" that would allow access to data by anyone other than the authorized user. Thus, the Commonwealth states, the files on the four computers cannot be accessed and viewed unless the authorized user first enters the correct password to unlock the encryption. The Commonwealth believes that evidence of the defendant's purported criminal activities is located on these computers.

On the day of his arrest, the defendant was interviewed by law enforcement officials after having been advised of the Miranda rights. In response to questioning, he said that he had more than one computer in his home. The defendant also informed the officials that "[e]verything is encrypted and no one is going to get to it." In order to decrypt the information, he would have to "start the program." The defendant said that he used encryption for privacy purposes, and that when law enforcement officials asked him about the type of encryption used, they essentially were asking for the defendant's help in putting him in jail. The defendant reiterated that he was able to decrypt the computers, but he refused to divulge any further information that would enable a forensic search.

On November 21, 2011, the Commonwealth filed its motion to compel decryption pursuant to Mass. R. Crim. P. 14 (a) (2), as

---

the algorithm, the data is rendered 'readable' again."

appearing in 442 Mass. 1518 (2004). It sought an order compelling the defendant's compliance with a "protocol" that the Commonwealth had established to obtain decrypted digital data.[10]

---

[10] The Commonwealth's "protocol" is as follows:

> "1. The defendant, in the presence of his counsel, shall appear at the Computer Forensics Laboratory of Massachusetts Attorney General Martha Coakley within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
>
> "2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
>
> "3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
>
> "4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
>
> "5. The defendant is expressly ordered not to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program;
>
> "6. The Commonwealth shall not view or record the password or key in any way; [and]
>
> "7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter."

At the hearing on the motion to compel decryption, the Commonwealth stated that it "would be seeking to introduce the fact of encryption in order to suggest consciousness of guilt."

As grounds for the motion, the Commonwealth stated that compelling the defendant to enter the key to encryption software on various digital media storage devices that had been seized by the Commonwealth was essential to the discovery of "material" or "significant" evidence relating to the defendant's purported criminal conduct. The Commonwealth further stated that its protocol would not violate the defendant's rights under either the Fifth Amendment to the United States Constitution or art. 12 of the Massachusetts Declaration of Rights.

In denying the Commonwealth's motion to compel decryption, the judge said that, on the one hand, the Commonwealth merely was requesting a sequence of numbers and characters that would enable it to access information on the computers, but that, on the other hand, the Commonwealth was asking for the defendant's help in accessing potentially incriminating evidence that the Commonwealth had seized. In the judge's view, there was merit to the defendant's contention that production of a password to decrypt the computers constituted an admission of knowledge, ownership, and control. Further, the judge continued, the scenario presented in this case was far different from compelling a defendant to provide a voice exemplar, a handwriting exemplar, or a blood sample, all of which are deemed to be nontestimonial. The judge said that the defendant's refusal to disclose the encryption key during his interview with law enforcement officials could be construed as an invocation of his rights under the Fifth Amendment and art. 12. Finally, it was the judge's

understanding that neither the Federal nor the State Constitution requires a defendant to assist the government in understanding evidence that it has seized from a defendant.

2. Decryption under the Fifth Amendment. The Commonwealth contends that compelling the defendant to enter his encryption key into the computers pursuant to the Commonwealth's protocol would not violate the defendant's Fifth Amendment right against self-incrimination. In the Commonwealth's view, the defendant's act of decryption would not communicate facts of a testimonial nature to the government beyond what the defendant already has admitted to investigators. As such, the Commonwealth continues, the defendant's act of decryption does not trigger Fifth Amendment protection. We agree.[11]

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[12] See Couch v. United States, 409 U.S. 322, 328 (1973) ("It is extortion of information from the accused himself that

---

[11] Generally speaking, "discovery matters are committed to the sound discretion of the trial judge." Buster v. George W. Moore, Inc., 438 Mass. 635, 653 (2003). "We will uphold discovery rulings unless the appellant can demonstrate an abuse of discretion that resulted in prejudicial error." Id., citing Solimene v. B. Grauel & Co., 399 Mass. 790, 799 (1987). However, we review a judge's rulings on mixed questions of fact and law de novo. See McCarthy v. Slade Assocs., 463 Mass. 181, 190 (2012); Commissioner of Revenue v. Comcast Corp., 453 Mass. 293, 303 (2009).

[12] In Malloy v. Hogan, 378 U.S. 1, 8 (1964), the United States Supreme Court held that the Fifth Amendment privilege against self-incrimination applies to the States through the Fourteenth Amendment to the United States Constitution. See Commonwealth v. Simon, 456 Mass. 280, 285 n.4, cert. denied, 131 S. Ct. 181 (2010).

offends our sense of justice"). It is well established that "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating" (emphasis in original). Fisher v. United States, 425 U.S. 391, 408 (1976). See United States v. Hubbell, 530 U.S. 27, 34 (2000) ("The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character"); Schmerber v. California, 384 U.S. 757, 761 (1966) ("[T]he privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature"). See also Commonwealth v. Hughes, 380 Mass. 583, 588, cert. denied, 449 U.S. 900 (1980).

Here, the Commonwealth, through its motion, is seeking to compel the defendant to decrypt "all" of the "digital storage devices that were seized from him." Given that the Commonwealth believes that those devices contain information about the defendant's alleged mortgage payoff scheme, the entry of the encryption key or password presumably would be incriminating because "it would furnish the Government with a link in the chain of evidence leading to [the defendant's] indictment." Doe v. United States, 487 U.S. 201, 207 n.5 (1988), and accompanying text. The issue on which this case turns is whether the defendant's act of decrypting the computers is a testimonial

communication that triggers Fifth Amendment protection.

Although the Fifth Amendment privilege typically applies to oral or written statements that are deemed to be testimonial, United States v. White, 322 U.S. 694, 698 (1944), the act of producing evidence demanded by the government may have "communicative aspects" that would render the Fifth Amendment applicable. Fisher, 425 U.S. at 410. See Hubbell, 530 U.S. at 36. See also Commonwealth v. Burgess, 426 Mass. 206, 211 (1997) ("The Fifth Amendment privilege against self-incrimination applies not only to verbal communications, but . . . also to nonverbal acts that imply assertions"). Whether an act of production is testimonial depends on whether the government compels the individual to disclose "the contents of his own mind" to explicitly or implicitly communicate some statement of fact. Hubbell, supra at 43, quoting Curcio v. United States, 354 U.S. 118, 128 (1957). See Doe v. United States, 487 U.S. at 213 (Fifth Amendment intended "to spare the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government"). See also Pennsylvania v. Muniz, 496 U.S. 582, 595 n.9 (1990) (opinion of Brennan, J.) ("nonverbal conduct contains a testimonial component whenever the conduct reflects the actor's communication of his thoughts to another"). More particularly, the act of complying with the government's demand could constitute a testimonial communication where it is considered to be a tacit admission to the existence of the

evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence. See Hubbell, supra at 36 & n.19; United States v. Doe, 465 U.S. 605, 613-614 & n.11 (1984); Fisher, supra. See also Commonwealth v. Burgess, supra; Commonwealth v. Hughes, 380 Mass. at 592. The determination whether an act of producing evidence in response to a governmental demand is sufficiently testimonial that it renders the Fifth Amendment applicable "depend[s] on the facts and circumstances of [each] particular case[]." Fisher, supra. See Doe v. United States, 487 U.S. at 214-215.

It is well established that not all acts of production have communicative aspects such that they will be deemed testimonial. See Hubbell, 530 U.S. at 34-35; Doe v. United States, 487 U.S. at 210-211. Significantly, the Fifth Amendment privilege is not triggered where the government seeks to compel an individual to be the source of real or physical evidence by, for example, furnishing a blood sample, Schmerber v. California, 384 U.S. at 764-765; producing a voice exemplar, United States v. Dionisio, 410 U.S. 1, 5-7 (1973); standing in a lineup, United States v. Wade, 388 U.S. 218, 221-223 (1967); providing a handwriting exemplar, Gilbert v. California, 388 U.S. 263, 266-267 (1967); or putting on particular clothing, Holt v. United States, 218 U.S. 245, 252-253 (1910). See Commonwealth v. Brennan, 386 Mass. 772, 776-777 (1982) (breathalyzer test and field sobriety tests do not produce evidence of testimonial nature). The Fifth Amendment privilege is not implicated in these circumstances because the

individual is "not required 'to disclose any knowledge he might have,' or 'to speak his guilt.'" Doe v. United States, supra at 211, quoting United States v. Wade, supra at 222-223. See Hubbell, supra at 35 ("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"); Pennsylvania v. Muniz, 496 U.S. at 590-599 (discussing distinctions between production of "real or physical" evidence and production of "testimonial" communication for purposes of privilege against self-incrimination).

Here, the defendant's act of entering an encryption key in the computers seized by the Commonwealth would appear, at first blush, to be a testimonial communication that triggers Fifth Amendment protection. By such action, the defendant implicitly would be acknowledging that he has ownership and control of the computers and their contents.[13] This is not simply the production of real or physical evidence like a blood sample or a handwriting exemplar. Rather, the defendant's act of entering the encryption key would be a communication of his knowledge

[13] Because the actual files and documents that are located on the defendant's computers were voluntarily created by the defendant in the course of his real estate dealings, they are not testimonial communications that enjoy Fifth Amendment protection. See United States v. Hubbell, 530 U.S. 27, 35-36 (2000) (recognizing "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 [Fifth Amendment] privilege"); United States v. Doe, 465 U.S. 605, 611-612 (1984); Fisher v. United States, 425 U.S. 391, 409-410 (1976).

about particular facts that would be relevant to the Commonwealth's case. Our analysis, however, does not end here. We must further determine whether the defendant's act of production loses its testimonial character because the information that would be disclosed by the defendant is a "foregone conclusion."

The "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, such that the individual "adds little or nothing to the sum total of the Government's information." Fisher, 425 U.S. at 411. For the exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence. See id. at 410-413; United States v. Bright, 596 F.3d 683, 692 (9th Cir. 2010). See also Hubbell, 530 U.S. at 40-41, 44-45 (government did not satisfy "foregone conclusion" exception where no showing of prior knowledge of existence or whereabouts of documents ultimately produced by respondent to subpoena); United States v. Doe, 465 U.S. at 613-614 & nn.11-13 (act of producing business records involved testimonial self-incrimination where government did not show that existence, possession, and authenticity of records were "foregone conclusion"). In those instances when the government produces evidence to satisfy the "foregone conclusion" exception, "no

constitutional rights are touched. The question is not of testimony but of surrender." Fisher, supra at 411, quoting Matter of Harris, 221 U.S. 274, 279 (1911). See, e.g., United States v. Sideman & Bancroft, LLP, 704 F.3d 1197, 1202-1205 (9th Cir. 2013) (quantum of information possessed by Internal Revenue Service regarding existence and possession of summonsed documents, together with evidence of their authenticity, satisfied "foregone conclusion" exception to Fifth Amendment privilege against self-incrimination); United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (Fifth Amendment not implicated by requiring production of unencrypted contents of computer where government knew of existence and location of files, although not specific content of documents, and knew of defendant's custody or control of computer); State v. Jancsek, 302 Or. 270, 287-288 (1986) (compelled production of letter not protected by Fifth Amendment privilege where existence, contents, and authenticity of letter already known to police). In essence, under the "foregone conclusion" exception to the Fifth Amendment privilege, the act of production does not compel a defendant to be a witness against himself.

Based on our review of the record, we conclude that the factual statements that would be conveyed by the defendant's act of entering an encryption key in the computers are "foregone conclusions" and, therefore, the act of decryption is not a testimonial communication that is protected by the Fifth Amendment. The investigation by the corruption, fraud, and

computer crime division of the Attorney General's office uncovered detailed evidence that at least two mortgage assignments to Baylor Holdings were fraudulent. During his postarrest interview with State police Trooper Patrick M. Johnson, the defendant stated that he had performed real estate work for Baylor Holdings, which he understood to be a financial services company. He explained that his communications with this company, which purportedly was owned by Russian individuals, were highly encrypted because, according to the defendant, "[that] is how Russians do business." The defendant informed Trooper Johnson that he had more than one computer at his home, that the program for communicating with Baylor Holdings was installed on a laptop, and that "[e]verything is encrypted and no one is going to get to it." The defendant acknowledged that he was able to perform decryption. Further, and most significantly, the defendant said that because of encryption, the police were "not going to get to any of [his] computers," thereby implying that all of them were encrypted.

When considering the entirety of the defendant's interview with Trooper Johnson, it is apparent that the defendant was engaged in real estate transactions involving Baylor Holdings, that he used his computers to allegedly communicate with its purported owners, that the information on all of his computers pertaining to these transactions was encrypted, and that he had the ability to decrypt the files and documents. The facts that would be conveyed by the defendant through his act of decryption

-- his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key -- already are known to the government and, thus, are a "foregone conclusion."[14] The Commonwealth's motion to compel decryption does not violate the defendant's rights under the Fifth Amendment because the defendant is only telling the government what it already knows.

3. Decryption under art. 12. The Commonwealth also contends that compelling the defendant to enter his encryption key pursuant to the Commonwealth's protocol would not violate his privilege against self-incrimination under art. 12 of the Massachusetts Declaration of Rights. We agree.

Article 12 provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself." It is well established that art. 12 affords greater protection against self-incrimination than does the Fifth Amendment in circumstances that are "discrete and well defined."[15] Commonwealth v. Burgess,

---

[14] We note that compliance with an order for the production of specific documents pursuant to a subpoena may be deemed to be a testimonial communication of the fact that the documents produced are the ones demanded, thereby constituting authentication of those documents. See Fisher v. United States, 425 U.S. at 412-413 & n.12. Here, the defendant's decryption of his computers does not present an authentication issue analogous to that arising from a subpoena for specific documents because he is not selecting documents and producing them, but merely entering a password into encryption software.

[15] We have held, for example, that art. 12 of the Massachusetts Declaration of Rights does not allow a defendant's refusal to submit to a breathalyzer test to be admitted in evidence. Compare Opinion of the Justices, 412 Mass. 1201, 1209-1211 (1992), with South Dakota v. Neville, 459 U.S. 553, 562-564 (1983). We also have held that a custodian of corporate records

426 Mass. at 218. See Commonwealth v. Mavredakis, 430 Mass. 848, 858-859 (2000). However, as we have explained, "[a]lthough art. 12 demands a more expansive protection, 'it does not change the classification of evidence to which the privilege applies. Only that genre of evidence having a testimonial or communicative nature is protected under the privilege against self-incrimination.'" Commonwealth v. Burgess, supra, quoting Attorney Gen. v. Colleton, 387 Mass. 790, 796 n.6 (1982). Like the Federal Constitution, the protection against self-incrimination afforded by art. 12 is unavailable where the government seeks to compel an individual to be the source of real or physical evidence. See Commonwealth v. Burgess, supra, and cases cited.

Similarly, we have held that, as is the case under the Federal Constitution, "the act of production, quite apart from the content of that which is produced, may itself be communicative." Commonwealth v. Doe, 405 Mass. 676, 679 (1989). See Commonwealth v. Hughes, 380 Mass. at 592. Where the information conveyed by an act of production "is reflective of

---

may invoke his art. 12 right against self-incrimination in response to a subpoena for those records where the act of production itself would be personally incriminating. Compare Commonwealth v. Doe, 405 Mass. 676, 678 (1989), with Braswell v. United States, 487 U.S. 99, 108-110 (1988). Additionally, we have held that the type of immunity that provides the requisite degree of protection for art. 12 purposes is so-called transactional immunity, which affords broader protection that the "use and derivative use immunity" required by the Fifth Amendment. Compare Attorney Gen. v. Colleton, 387 Mass. 790, 795-801 & n.4 (1982), with Kastigar v. United States, 406 U.S. 441, 453 (1972).

the knowledge, understanding, and thoughts of the witness," it is deemed to be testimonial and, therefore, within the purview of art. 12. Commonwealth v. Doe, supra. At the same time, we also have recognized that "[w]hen it is a 'foregone conclusion' that a witness has certain items, and the items themselves are not privileged, the witness has no privilege." Id. at 680-681, citing Commonwealth v. Hughes, supra at 590, and Fisher v. United States, 425 U.S. at 411. See Commonwealth v. Diaz, 383 Mass. 73, 76 n.5 (1981) (no serious constitutional issue of self-incrimination raised by disclosure of information that is "foregone conclusion"). See also note 13, supra.

In Commonwealth v. Burgess, 426 Mass. at 219, when the court considered the scope of the protection against self-incrimination afforded by both the Federal Constitution and the Massachusetts Declaration of Rights, we pointed out that our analysis under art. 12 need not "merely duplicate our earlier Fifth Amendment analysis." Rather, "[w]e are free to consider certain evidence, considered by the Supreme Court to be insufficiently testimonial for Fifth Amendment purposes, to be sufficiently testimonial for art. 12 purposes." Id. Mindful of this pronouncement, as well as our jurisprudence recognizing the "foregone conclusion" principle, we are not persuaded that the circumstances presented here dictate an analytical departure from the Federal standard. Where the facts that would be conveyed by the defendant through the act of entering an encryption key into the computers seized by the Commonwealth are a "foregone conclusion," his act of

production is insufficiently testimonial for art. 12 purposes.[16]

4. Conclusion. We answer the reported question, "Yes, where the defendant's compelled decryption would not communicate facts of a testimonial nature to the Commonwealth beyond what the defendant already had admitted to investigators." The judge's denial of the Commonwealth's motion to compel decryption is reversed, and this case is remanded to the Superior Court for further proceedings consistent with this opinion.

So ordered.

[16] As properly enunciated by the Commonwealth in its protocol, see note 10, supra, the compelled act of computer decryption cannot be used to prove that the defendant had custody and control over the computers. Cf. Commonwealth v. Burgess, 426 Mass. 206, 220 (1997).

LENK, J (dissenting, with whom Duffly, J., joins). The court holds today that the defendant, an attorney who practices from his home, may be ordered to enter decryption keys sequentially on each and every electronic device seized from his home, his home office, and his automobile, in order to provide law enforcement officers with unencrypted access to those devices.[1] Such an order is the functional equivalent of requiring him to produce the unencrypted contents of the devices seized. The government suspects that some unspecified set of documents related to a mortgage fraud scheme may be located on one or more of these devices,[2] which the government thus far has

[1] The Commonwealth's proposed order requires the defendant to decrypt "all" of the "digital storage devices that were seized from him." These include two desktop computers and a laptop computer seized from his house; a "netbook" computer seized from his automobile; an external hard drive; two universal serial bus (USB) "thumb" drives (also known as "flash drives," "USB drives," and "sticks"); fourteen compact discs; two secure digital cards; and two cellular telephones. The devices were seized pursuant to a search warrant issued based on an affidavit by a State trooper involved in the investigation. The affidavit sought, inter alia, "[c]omputers and/or electronic storage devices capable of storing any of the below-described records and/or data"; it encompassed "[a]ny and all records, documents, items, and/or data, in whatever form, relating in any way to" a lengthy list of broadly defined items.

[2] A "netbook" is a smaller, more lightweight, and less powerful type of laptop computer usually used for Internet and electronic mail (e-mail) access. See Cloud Control: Copyright, Global Memes and Privacy, 10 J. Telecomm. & High Tech. L. 53, 58 & n.27 (2012). Flash drives "are solid state memory devices that can comfortably be carried on a key chain. They can be used, usually thru a USB port, much like an external hard drive." United States v. Burgess, 576 F.3d 1078, 1090 n.12 (10th Cir.), cert. denied, 558 U.S. 1097 (2009). Like flash drives, secure digital cards are a type of "solid-state memory technology that stores information when not powered," but they "serve different functions and have limitations that USB flash drives do not"; secured digital cards "are thin cards used in phones or cameras

been unable to read because of the encryption. I agree with the court that this act of decryption is compelled, testimonial, and potentially incriminating. Unlike the court, I conclude that this also holds true for the intrinsically linked act of thereby producing in unencrypted form any material that may be on the now encrypted devices. Further, I do not agree that the Commonwealth has shown sufficient knowledge of the existence, location, and authenticity of the documents it seeks such that the information that would be revealed by decryption and production is a "foregone conclusion," and therefore that requiring the defendant to decrypt the devices would not violate his constitutional privilege against self-incrimination. Because I believe that the act of compelled entry of the codes to decrypt the seized devices, thereby producing the unencrypted contents of those devices, is protected under both the Fifth Amendment to the United States Constitution and art. 12 of the Massachusetts Declaration of Rights, I respectfully dissent.

1. Act of production and authentication. The court concludes that the act of decrypting the devices pursuant to the Commonwealth's proposed protocol, which necessarily would produce in unencrypted form any files stored thereon to which the encryption key would permit access, is not analogous to the act of responding to a subpoena to produce a document, where the act

---

that serve primarily as digital film substitutes." Sandisk Corp. v. Kingston Tech. Co., 863 F. Supp. 2d. 815, 819-820 (W.D. Wis. 2012). They are "not readily compatible with computers and often require a special adaptor to interface with a computer's USB port." Id. at 820.

of production would be testimonial because it makes an assertion that, among other things, the document produced is authentic. To reach this conclusion, the court adopts the Commonwealth's contention that, by decrypting the computers and thereby producing their unencrypted contents, the defendant would be asserting only his ability to decrypt the devices. On this view, he would not be asserting that he owned them, had exclusive use and control of them, or was familiar with any of the files on them; that certain files contained the incriminating evidence sought; or that the documents were authentic. Such is far from the case.

In taking this view of the matter, the court maintains that the defendant merely would be entering a password, which he would not disclose to the Commonwealth, into the encryption program, and would not thereby be selecting and producing any documents. Such an artificial distinction between the act of entering the decryption key and the inevitable result of decrypting the devices,[3] and thereby producing the files for inspection, obfuscates the reality of what the defendant is being compelled to disclose. The Commonwealth seeks the decryption order at issue not for its own sake, but rather to enable the government to access the documents it sought when obtaining the search

---

[3] That no individual file would be decrypted on the computer's disk drive until someone requested that particular file is of no moment. According to the Commonwealth's expert, the act of entering the decryption key is what would permit the decryption program to run automatically and provide readable access to an individual file upon request.

warrant permitting it to seize the devices. Here, as the United States Court of Appeals for the Eleventh Circuit concluded in similar circumstances, "the decryption and production would be tantamount to testimony by [the defendant] 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." In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (2012) (In re Subpoena Duces Tecum). Inexorably, once the decryption key is entered, the names and sizes of the files (if any) to which the defendant has access on that computer will be produced, the amount of unused space available to the defendant on that computer will become known, and the contents of any files will be made accessible to the Commonwealth.[4]

Moreover, the defendant has denied that there are any documents related to Baylor Holdings, Ltd. (Baylor), on that subset of the seized devices of which he has acknowledged ownership, denied that he created any documents for Baylor,[5] denied that the encrypted communication program he used to communicate with Baylor continues to be installed on those

[4] The issue, of course, is not whether the decrypted contents of the computer are "testimonial," but whether the act of decrypting the computer and thereby producing decrypted information is "testimonial" under the Fifth Amendment to the United States Constitution and art. 12 of the Massachusetts Declaration of Rights.

[5] The defendant told police that he received the already-executed mortgage assignment documents from Baylor through the United States mail, and that he merely recorded those documents at the relevant registry of deeds.

devices, and denied that there are any saved records of the encrypted communications he had with Baylor employees. If the defendant is compelled to decrypt the devices, and any such documents are produced thereby, the act of decryption will have resulted in a prior inconsistent statement by the defendant, which the Commonwealth may seek to use against him at trial.[6]

---

[6] The Commonwealth asserts that while, according to the proposed "protocol," it will not introduce evidence of the manner in which the computers were decrypted (unless the defendant opens the door), it intends to introduce evidence of the encryption itself as evidence of "consciousness of guilt." The Commonwealth intends to make this argument even though encrypting files on computers is now a common business practice that is mandatory in many circumstances. See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1347 (2012) (rejecting "the suggestion that simply because the devices were encrypted necessarily means that [the defendant] 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"). See also G. L. c. 93H, § 2 (requiring adoption of regulations "relative to any person that owns or licenses personal information about a resident of the commonwealth" that are designed to "insure the security and confidentiality" of such information; "protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information"); 201 Code Mass. Regs. §§ 17.00 (2009) (implementing G. L. c. 93H); G. Jacobs & K. Laurence, Professional Malpractice § 17.1 (2013) (discussing requirement, pursuant to G. L. c. 93H and Supreme Judicial Court Interim Guidelines for Protection of Personal Identifying Data, that attorneys "identify reasonably foreseeable risks to records containing such information, control access to it, establish policies regarding storage and secure transportation of records [e.g., in e-mail correspondence] outside of the premises, require use of up-to-date computers, firewalls, anti-virus software, and secure encryption of all electronically stored and transported data" [emphasis supplied]); John W. Sime, Selecting a Law Firm Cloud Provider, 93 Mich. B.J. 48, 49 (2013) ("Data should be encrypted at two stages. The first stage is during data transmission. . . . [D]ata should also be encrypted while in storage at the cloud provider"). Moreover, it also seems likely, and the Commonwealth has not stated otherwise, that, should any such documents be produced on any of the seized devices, the Commonwealth will seek to characterize evidence of the

In light of all this, I would conclude that both the acts of decrypting the devices and of inexorably producing thereby the unencrypted contents of the devices that the Commonwealth otherwise cannot now access are testimonial. See United States v. Hubbell, 530 U.S. 27, 43 (2000) (Hubbell); Doe v. United States, 487 U.S. 201, 212 (1988).

2. Foregone conclusion. The court concludes that the act of entering the codes to decrypt the devices would not infringe upon the defendant's privilege against self-incrimination. The court is of the view that the defendant already has disclosed during an interview with State troopers anything that, absent such disclosures, might be testimonial about the act of decryption. In particular, the court concludes that the facts which might be learned through the act of decryption -- ownership and control of the seized devices -- have been revealed previously by the defendant, or are already known by the Commonwealth through other means, and therefore that the "foregone conclusion" exception applies to what otherwise would be testimonial conduct. The court does not consider whether the act of production, also in my view testimonial, is encompassed within the foregone conclusion exception.

"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

---

defendant's earlier denials as inconsistent statements, lies, and further consciousness of guilt.

communicate some statement of fact." In re Subpoena Duces Tecum, 670 F.3d at 1345, quoting Curcio v. United States, 354 U.S. 118, 128 (1957). Under the foregone conclusion doctrine, an otherwise testimonial act of production is not testimonial if the government establishes that, at the time it sought the compelled production, it already knew of that which would explicitly or implicitly be conveyed by the production. Fisher v. United States, 425 U.S. 391, 410-411 (1976) (Fisher). See Hubbell, supra at 36 n.19, 43-45 (act of production testimonial if by compelled conduct "the witness would admit that the papers existed, were in his possession or control, and were authentic"; inquiry turns on extent of government's prior knowledge of existence and location of documents produced); United States v. Ponds, 454 F.3d 313, 320-321 (D.C. Cir. 2006).

a. Reasonable particularity standard. In addressing the extent of knowledge that the government must establish in order to invoke the "foregone conclusion" doctrine, four circuit courts of the United States Court of Appeals have concluded that the government must show with "reasonable particularity" that it already knows the "location, existence, and authenticity of the purported evidence." In re Subpoena Duces Tecum, 670 F.3d at 1344 & n.20. See United States v. Ponds, supra at 320-321; In re Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004); In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993), cert denied sub nom. Doe v. United States, 510 U.S. 1091 (1994).

Treating computer files as documents, the United States Court of Appeals for the Eleventh Circuit is, to date, the only circuit court to have addressed the issue specifically in the context of encrypted computers. Concluding that a defendant's compelled decryption and production of the contents of computer drives and external hard drives would be sufficiently testimonial to trigger Fifth Amendment protections, the court determined that "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.'" In re Subpoena Duces Tecum, 670 F.3d at 1345-1346. To establish a foregone conclusion, "[t]he government does not have to show that it knows specific file names," but would have to "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." Id. at 1349 n.28.

While the United States Court of Appeals for the First Circuit has yet to consider the issue, I would adopt, at a minimum for purposes of art. 12, the same reasonable particularity standard for establishing a foregone conclusion that other circuit courts have adopted, and would conclude that

the Commonwealth has not met that burden here. See id. at 1346, 1349 (no evidence "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"). Contrast United States v. Fricosu, 841 F. Supp. 2d 1232, 1235-1237 (D. Colo. 2012) (existence and location of files foregone conclusion where government introduced recorded conversation of defendant and third party in which she said that file sought "was on my laptop").

b. Extent of government's knowledge in this case. Here, the Commonwealth has made no showing that the existence, possession, and authenticity of the broad categories of items sought are foregone conclusions, under any definition of that term. The court focuses on the defendant's apparent access to the devices seized, and his statements that he owns a "laptop," that "everything is encrypted," and that he could decrypt at least one device ("my computer"). In so doing, it conflates the probable cause showing that the Commonwealth was required to make in order to seize the devices in the first instance with the showing that the Commonwealth must make when, as here, it seeks the otherwise testimonial assistance of a defendant in accessing the contents of those devices.[7] The showing that the

[7] The Commonwealth argues that the order to provide the key to decrypt the computers and thereby produce the unencrypted documents is necessary because encryption creates significant difficulties for law enforcement officers attempting to prosecute a lengthy list of serious crimes. In a similar vein, the Commonwealth argues explicitly that it should be able to compel the decryption of the devices and the production of their content

Commonwealth must make as to its knowledge of the contents of those devices in order to render anything revealed by the decryption and production of that content a foregone conclusion is significantly greater than what is required to show probable cause. Hence, the "reasonable particularity" standard requires much more than government knowledge that a defendant owns or has access to a particular computer.

Even under the less specific requirements articulated in Hubbell, supra, moreover, the government's burden of establishing that, at the time it sought to compel decryption and production, it already knew of the documents sought, rendering any testimonial aspect of that conduct a foregone conclusion, is not met by a showing that a defendant had in his house what is essentially a locked file cabinet in which such documents might

---

based on the warrant affidavit, which established probable cause to seize them, as the seizure otherwise has produced no information that would be useful in prosecuting the charged offenses.

It does not follow, however, that further restrictions should be placed on fundamental protections provided by the Fifth Amendment and art. 12, which heretofore have been enforced by both State and Federal courts, because the prevalence of computers, in this digital age, at times may facilitate the commission of crimes. The omnipresence of electronic devices which may be monitored, tracked, and recorded has likewise afforded unparalleled opportunities to law enforcement officers in their pursuit of criminal investigations. That encryption may at times present significant difficulties to law enforcement officers does not, as the Commonwealth suggests, result in a conclusion that the Fifth Amendment privilege should be restricted so that enforcement is made easier. See Blaisdell v. Commonwealth, 372 Mass. 753, 761 (1977) ("Where the privilege is applicable, the constitutionally required result is that no balancing of State-defendant interests is permissible to facilitate the admittedly difficult burdens of the prosecution"). See also Commonwealth v. Doe, 405 Mass. 676, 680 (1989).

have been kept. See In re Subpoena Duces Tecum, 670 F.3d at 1347 n.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").

i. Existence and content of documents sought. Aside from knowledge pertinent to the existence and nature of the encryption program itself,[8] the government has not shown that it has any knowledge as to the existence or content of any particular files or documents on any particular computer.[9] To the contrary, the Commonwealth's computer forensic expert's affidavit provides general information about what computers can do, but makes no specific assertions as to any files or documents expected to be found on any of the seized devices. The focus of the trooper's affidavit is on the defendant's actions away from his home, as

[8] David Papargiris, the director of the Attorney General's computer forensics laboratory, submitted an affidavit in support of the Commonwealth's motion to compel decryption. Papargiris stated that some of the storage devices seized from the defendant's house indicate use of an encryption program called "DriveCrypt Plus Pack." When this program is installed on a computer, the computer displays a particular screen requesting a password every time the computer is started. Nothing further can be done on that computer until the user enters the password. Because all of the seized computers display the same screen when they are started, Papargiris believes that the program is being used for all of the seized computers and separate storage devices.

[9] As to one external hard drive, the Commonwealth has shown knowledge of two documents related to the defendant's own home, not involving Baylor Holdings, Ltd. (Baylor), or Puren Ventures, Inc., and some links (which do not involve documents) to third-party Web sites.

observed by police surveillance.[10] Not only is there no description of files that are expected to be found,[11] let alone that are known to exist, on the defendant's computers,[12] the

[10] The trooper's affidavit details police surveillance and review of surveillance video footage of the defendant driving to various stores and post offices. Police suspect the defendant purchased money orders and gift cards at these locations, by filling out forms by hand. Additional surveillance footage shows the defendant on one occasion entering and leaving a court house that also houses a registry of deeds. Cooperating witnesses and documents obtained from third parties indicate that an unknown individual purporting to represent Baylor arranged for checks to be mailed via United States mail to the defendant's former office building in Boston.

The affidavit also recounts police observations of the defendant suspected to be using publicly available and "anonymous" wireless Internet services, which allow access to the Internet without identifying a particular user's Internet Protocol (IP) address, from a variety of locations, such as restaurants. These suspicions are based largely on his presence at particular times at locations where such services are available, or in nearby parking lots, and, on two occasions, because he was observed apparently using a laptop.

[11] Based on the affidavits, the Commonwealth clearly had probable cause to seize the devices themselves. In this regard, there was reason to think the defendant used some unspecified computer to connect to the Internet in communicating with the intended victims of the fraud.

[12] The search warrant affidavit states that the seized computers "are capable of storing," inter alia, information about the defendant's "contacts and activities" for a period of more than four months, "anything having do to with" his financial transactions over an approximately three-year period (although the fraudulent mortgage scheme allegedly lasted for less than one year), any Internet search, over an unlimited time frame and geographic area, for residential properties, and "any" document filed with "any Massachusetts Registry of Deeds," again over an unlimited period. The same information is also sought, from "[a]ny and all records, documents, items, and/or data, in whatever form," to be found at the defendant's house and in his automobile. The affidavit states further that, because "[t]ransferring data files between computers or onto storage devices such as disks is a simple task that takes little time . . . once a file is on one computer at a given location -- particularly a home -- I believe that there is probable cause to

affidavit contains numerous indications of the defendant's apparent efforts to avoid downloading documents to his computers, using telephone or facsimile transmission from his house. Service providers' Web sites that the Commonwealth asserts the defendant used,[13] are described as advertising that documents are stored on the third-party service providers' computers, and may be accessed over the Internet without downloading anything to a user's own computer. See G. Jacobs & K. Laurence, Professional Malpractice § 17.1 (2013) (discussing "cloud computing" as "in

---

believe that it could be moved to any storage device or other computer at that same location." The court does not address whether these broad categories and date ranges meet the specificity requirements of Commonwealth v. McDermott, 448 Mass. 750, 771-775, cert. denied, 552 U.S. 910 (2007) (concluding that each computer file is separate, closed container, and discussing limitations necessary on searches to be conducted of computer hard drives so that warrants to conduct such searches are not constitutionally infirm). The record here also does not indicate whether the Commonwealth sought a warrant as to the search of each of the devices once they had been seized and transported to the police laboratory. See id. at 774-775.

[13] The trooper's affidavit suggests that the defendant made use of third-party services over the Internet to establish certain corporate telephone and facsimile numbers The Web sites described in the affidavit, however, are explicitly discussed as services which would not require placing any documents on a suspect's own computer. They are described as permitting anonymous use, storing documents on the third-party service provider's computers, and permitting access to, for instance, e-mail message attachments without downloading anything to a user's own computer. See United States v. Falso, 544 F.3d 110, 112-114 (2d Cir. 2008) (warrant affidavit asserting after forensic examination of computer that defendant "appeared to have gained or attempted to gain" access to Web site which distributed and sold child pornography, where e-mail address belonging to defendant was listed as subscriber to member section of Web site, defendant had Internet service from his house, and defendant had been convicted of prior misdemeanor sex offense, did not establish probable cause that images of child pornography would be found on defendant's computer).

essence a sophisticated form of remote electronic data storage on the Internet. . . . Unlike traditional methods that maintain data on a computer or service at a law office or other place of business, data stored 'in the cloud' [cloud computing] is kept on large servers located elsewhere and maintained by a vendor"). The Commonwealth accordingly has not shown that it knows "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." In re Subpoena Duces Tecum, 670 F.3d at 1349 n.28.

"In Fisher, [supra at 411,] . . . 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[, supra at 44-45,] 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." In re Subpoena Duces Tecum, 670 F.3d at 1345. Here, too, the government has no more than a suspicion that broad categories of documents, extending over periods of years, may exist on one or more of the seized devices. See United States v. Doe, 465 U.S. 605, 613-614 & nn.11-13 (1984). See, e.g., Commonwealth v. Hughes, 380 Mass. 583, 592, cert. denied, 449 U.S. 900 (1980) (act of producing gun by defendant charged with assault by means

of dangerous weapon would not convey "merely trivial new knowledge" but would communicate "just those matters about which the Commonwealth desires but does not have solid information"). Contrast Fisher, supra.

The court notes that the defendant has admitted to engaging in real estate transactions for Baylor, communicating with Baylor over an encrypted communication program installed on his laptop, using the Internet to communicate, having more than one computer, that "everything" on his computer is encrypted, and that he knows how to decrypt it. The court points also to the fact that two of the mortgage assignments to Baylor apparently are fraudulent.[14] None of this, however, establishes anything about the government's knowledge of the documents, if any, that may be stored on the seized devices.[15] See In re Grand Jury Subpoena dated April 18, 2003, 383 F.3d at 910 ("Although the government possessed extensive knowledge about [defendant's] price-fixing activities as a result of interviews with cooperating witnesses and [his] own incriminating statements . . . , it is the

[14] Police suspect the two assignments to Baylor are fraudulent based on their communication with the closing attorneys involved in the sales of the two properties not long after the assignments had been recorded, and with the banks that previously held the mortgages.

[15] The trooper's affidavit states, without record support, that evidence seized from the external hard drive shows that the defendant used his computers to create the forged assignments. The documents described as having been observed on the external hard drive, however, which are the only specific documents described as existing on any of the seized devices, relate to an unsigned release of a mortgage on the defendant's own property, and not to any assignment to Baylor; nothing in the affidavit indicates how the documents were created.

government's knowledge of the existence and possession of the actual documents, not the information contained therein, that is central to the foregone conclusion inquiry").

Furthermore, the court misconstrues the extent of the defendant's statements concerning the encryption, thereby inferring that the defendant has asserted greater access and control than is in fact the case. The court conflates the encryption of the disk drive on one of the computers, which the defendant acknowledged, with the existence of the encrypted communication program[16] purportedly used to communicate with Baylor.[17] Contrary to the court's statement, the defendant has

---

[16] As the defendant described it to police, the communication program works like an online "chat" session; one person types, and the other person sees the message displayed on his or her computer screen. The message that the user types is encrypted before it is sent to the recipient. The program as described is not intended to create and store documents, or to encrypt computer drives, but, rather, to allow users to send messages back and forth in a secure way so that someone trying to eavesdrop on the messages being sent would be unable to do so.

[17] The court points to the defendant's statement to police that, "[i]n order to decrypt the information, he would have to 'start the program'" as being a reference to the "DriveCrypt" encryption software on the computer drives that it takes as an admission of control over the drives and the ability to decrypt them. The defendant was speaking, however, of the communication program he started in order to communicate in a "chat" session with the Russian individuals at Baylor, not of the encryption of the computer drives themselves. According to the defendant's statement, the communication program takes up very little space on a computer drive and can be installed on any device, including a removable "flash" drive; the program requires only an Internet connection, and can be run from anywhere, by inserting a "flash" drive into a computer.

The defendant, who is a native of Russia, obtained the program at a financial conference in Europe sometime in 2004, 2005, or 2006, because he intended to develop his business in the Russian market; he believed that encrypted communication was

not said that the communication program that he ran in order to communicate with someone at Baylor is installed on any of his computers at this time; indeed, he stated explicitly that it had been installed on his "laptop" but that it might no longer be there and that the program itself "may not exist anymore."[18]

On this record, the Commonwealth does not know what is stored on any of the seized devices, or if any of them contain information relevant to the charged offenses. Notwithstanding the court's conclusion to the contrary, the affidavit in support of the search warrant and the defendant's statements to police do not give rise to a foregone conclusion that whatever would be revealed by the defendant's entry of the decryption key, and consequent production of the unencrypted contents of all of the seized devices, is already known to the government. See Hubbell, supra at 45 ("the overbroad argument that a businessman . . . will always possess general business and tax records," could not "cure [the] deficiency" of government's failure to demonstrate

---

necessary to address Russian security concerns. In response to an explicit question, the defendant answered that he did not know whether the communication program saved the contents of any conversation on a computer drive, then clarified that the communication program did not save any of the typed conversations, but, rather, deleted them at the end of a communication session, and that he thought it did not store copies of the conversations because it was intended to be secure.

[18] When asked at another point about the location of the "encryption device" that he used to communicate with Baylor ("Is it on your laptop? Is it on your desktop"?) the defendant replied, "At different points it was." Whether the defendant was referring to the "laptop" seized from his house or the "netbook" seized from his car is unclear. It is also unclear which of the two other computers he meant by "your desktop."

its "prior knowledge of either the existence or the whereabouts" of requested documents); In re Grand Jury Subpoena Dated April 18, 2003, 383 F.3d at 911 ("A subpoena such as this, which seeks all documents within a category but fails to describe those documents with any specificity indicates that the government needs the act of production to build its case against [the defendant]"). See also United States v. Doe, 465 U.S. at 614 n.12.

Even more fundamentally, to establish a foregone conclusion the government must first show that it knows any files at all exist on a particular computer. In In re Subpoena Duces Tecum, 670 F.3d at 1346, 1349, the United States Court of Appeals for the Eleventh Circuit reversed an order requiring a suspect to decrypt his computer, which was using the same type of encryption program that the Commonwealth's expert avers is being used to encrypt the devices here, because the court concluded that the government had not shown that any files existed on the computer, other than the encryption program itself. The encryption program at issue not only encrypts information stored on a computer, it also encrypts all unused space on the computer's hard drive, making it impossible to determine how much of the computer contains actual files and how much is unused or blank. Because the government could not show that any data on the computer represented actual files, the court concluded that "[t]he [g]overnment has failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that

encrypted files exist on the drives . . ."). Id. at 1349. Given the properties of the encryption program in place on the seized devices here, as described by the Commonwealth's expert, the Commonwealth does not know whether they contain any documents of any kind.

ii. Ownership, exclusive use, and control. The court's decision also conflates access to a particular computer[19] with access to, and knowledge and control of, each of the files on that computer.[20] As stated, the United States Supreme Court has rejected the view that a defendant's access to a locked cabinet, whose contents are not known but that might contain the documents sought, is sufficient to establish that the government knows the contents of those documents, such that their compelled production

---

[19] The defendant stated that the computer in his home was in an area accessible to anyone in the house or who came to his home office, and that Baylor employees accessed his computer using the encrypted communication program. On this record, the government has not shown that the defendant had exclusive access to the computers.

[20] According to the Commonwealth's expert, the encryption program on the seized computers permits multiple users with distinct passwords, each potentially having access to a different portion of the computer drive. The government does not currently know how many user accounts exist on any of the computers, and to which portions, if any, of any particular computer the defendant has access. See Trulock v. Freeh, 275 F.3d 391, 403-404 (4th Cir. 2001) (where two individuals shared use of computer, and both had access to entire computer hard drive, other user did not have authority to consent to search of suspect's password-protected files on that drive). The ability to enter a password to start the computer does not, therefore, indicate whether the defendant has access to or control over all of the different user accounts and different sections of the computer drives that may have been established on any of the seized computers; it would, however, potentially reveal to the Commonwealth the existence of other accounts, and possibly others who use the computers, about which the Commonwealth has indicated no knowledge.

by unlocking the cabinet is a foregone conclusion. Hubbell, supra. This distinction is even more critical in considering the issue of production or search of files stored on a computer. See In re Subpoena Duces Tecum, 670 F.3d at 1346, 1349; United States v. Fricosu, 841 F. Supp. 2d 1232, 1235-1237 (D. Colo. 2012). Like many courts to have considered the issue, we have concluded that each computer file is a separate document in a closed container, requiring that searches of a computer to locate specific files must be limited and particular. See Commonwealth v. McDermott, 448 Mass. 750, 775, cert. denied, 552 U.S. 910 (2007). See United States v. Potts, 586 F.3d 823, 833 (10th Cir. 2009) ("officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant"). See, e.g., United States v. Mann, 592 F.3d 779, 786 (7th Cir.), cert. denied, 130 S. Ct. 3525 (2010), and cases cited; United States v. Burgess, 576 F.3d 1078, 1088-1089 (10th Cir.), cert. denied, 558 U.S. 1097 (2009); United States v. Carey, 172 F.3d 1268, 1270-1273 (10th Cir. 1999); United States v. Stierhoff, 477 F. Supp. 2d 423, 439 n.8 (D.R.I. 2007), aff'd, 549 F.3d 19 (1st Cir. 2008). See generally Goldfoot, The Physical Computer and the Fourth Amendment, 16 Berkeley J. Crim. L. 112 (2011); Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531 (2005); Trepel, Digital Searches, General Warrants, and the Case for the Courts, 10 Yale J. L. & Tech. 120 (2007). Therefore, the government must establish knowledge of the existence of the

particular file, either by the name of the file or by knowledge of its contents, as well as the defendant's access to that portion of the encrypted drive on which the file exists. See In re Subpoena Duces Tecum, 670 F.3d at 1346, 1349. It has not done so here.

3. Attorney-client privilege. I would conclude also that the defendant cannot be compelled to enter the decryption key, and thereby produce all documents to which he has access, on each device, under the protocol as proposed by the Commonwealth, because of the possibility that the computers contain privileged information relating to the defendant's legal clients. See Preventive Medicine Assocs. v. Commonwealth, 465 Mass. 810, 822-824 & nn.24-26 (2013) ("a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege . . . . [T]he harm to the defendant could be irreparable if the Commonwealth viewed privileged materials, even if only by accident"). The issue of attorney-client privilege is not addressed in the search warrant affidavit, the protocol proffered in conjunction with the Commonwealth's motion to compel, or the court's decision.[21]

[21] The question is addressed by the defendant in his brief and by the Commonwealth in its reply brief. While the Commonwealth asserts in its reply brief, prior to a discussion on the merits, that the question of attorney-client privilege is not part of the reported question before the court, the plain language of the Commonwealth's motion to report, which was allowed, and which is presented by the Commonwealth in its initial brief as "the issue presented for review," asks, "Can the defendant be compelled pursuant to the Commonwealth's proposed protocol to provide his key to seized encrypted digital evidence . . ." (emphasis supplied)? The joint stipulation of

The defendant told police that he ran a law office from his house, and that he had approximately ten active personal injury clients. He stated that he sent facsimile transmissions to his personal injury clients, when necessary, using TrustFax, an Internet facsimile site, from his home computer. He acknowledged that "my computer" is encrypted, but did not identify which one of the seized devices he meant, and asserted that the encryption was to protect his "privacy." The police photographs of one of the computer screens when that computer was running, showing the directory name "K:\Leon Documents\My Scans" and an icon labeled "Attorney Leon I. Gelfgatt," do not indicate that the documents, if any, on the computers relate to Baylor and not to the defendant's other clients. Nor do they show that the computers contain any documents related to Baylor. Because the proposed protocol potentially would allow the Commonwealth to view privileged information related to the defendant's other clients, I would conclude, on this basis as well, that the requested order to compel is unreasonable and impermissible.

4. Conclusion. Because I believe that the compelled decryption and production here is fundamentally testimonial, and the Commonwealth has not established a foregone conclusion that the existence, location, and authenticity of the information that would be produced is known to the government, I respectfully dissent, and would answer the reported question, "No."

---

the parties as to the wording of the reported question uses identical language.