Supreme Judicial Court of Massachusetts, Suffolk..
COMMONWEALTH
v.
Dennis JONES.

SJC-12564

Argued November 6, 2018

Decided March 6, 2019

Cellular Telephone. Witness, Compelling giving of evidence, Self-incrimination. Constitutional Law, Self-incrimination.

CIVIL ACTION commenced in the Supreme Judicial Court for the county of Suffolk on May 17, 2018.

The case was reported by Gants, C.J.

Attorneys and Law Firms

Gabriel Pell, Assistant District Attorney, for the Commonwealth.

James A. Reidy (George F. Ohlson, Jr., Stoneham, also present) for the defendant.

The following submitted briefs for amici curiae:

Andrew Levchuk & Lauren C. Ostberg, Springfield, for Orin S. Kerr.

David Rangaviz, Committee for Public Counsel Services, for Committee for Public Counsel Services.

Maura Healey, Attorney General, & Randall E. Ravitz, Assistant Attorney General, for the Attorney General.

Laurent Sacharoff, pro se.

Present: Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.

Opinion

KAFKER, J.

*1 A grand jury returned indictments charging the defendant, Dennis Jones, with trafficking a person for sexual servitude, G. L. c. 265, § 50 (a), and deriving support from the earnings of a prostitute, G. L. c. 272, § 7. At the time of his arrest, the Commonwealth seized a cell phone from the defendant. During its investigation of the defendant, the Commonwealth developed information leading it to believe that the contents of the cell phone included material and inculpatory evidence. The Commonwealth thereafter applied for and was granted a search warrant to search the cell phone. The search warrant has yet to be executed, however, as the Commonwealth was -- and currently remains -- unable to access the cell phone's contents because they are encrypted. The contents can only be decrypted with the entry of a password.[1]

The Commonwealth sought to compel the defendant to decrypt the cell phone by filing a motion for an order requiring the defendant to produce a personal identification number access code in the Superior Court. The central legal issue concerned whether compelling the defendant to enter the password to the cell phone would violate his privilege against self-incrimination guaranteed by both the Fifth Amendment to the United States Constitution and art. 12 of the Massachusetts Declaration of Rights. The Commonwealth argued that under our decision in Commonwealth v. Gelfgatt, 468 Mass. 512, 11 N.E.3d 605 (2014), the act of entering the password would not amount to self-incrimination because the defendant's knowledge of the password was already known to the Commonwealth, and was therefore a “foregone conclusion” under the Fifth Amendment and art. 12. Following a hearing, a judge denied the Commonwealth's motion, concluding that the Commonwealth had not proved that the defendant's knowledge of the password was a foregone conclusion under the Fifth Amendment.

Several months later, the Commonwealth renewed its motion and included additional factual information that

it had not set forth in its initial motion. The judge denied the renewed motion, noting that because the additional information was known or reasonably available to the Commonwealth when the initial motion was filed, he was "not inclined" to consider the renewed motion under the Massachusetts Rules of Criminal Procedure. The judge concluded that even if he were to consider the renewed motion, the Commonwealth had still failed to prove that the defendant's knowledge of the password was a foregone conclusion.

The Commonwealth then filed a petition for relief in the county court, pursuant to G. L. c. 211, § 3; the single justice reserved and reported the case to the full court. The single justice asked the parties to address three specific issues, in addition to any other questions they thought relevant. Those issues are the following:

*2 "1. What is the burden of proof that the Commonwealth bears on a motion like this in order to establish a 'foregone conclusion,' as that term is used in Commonwealth v. Gelfgatt, 468 Mass. 512, 520-526, 11 N.E.3d 605 (2014)?

"2. Did the Commonwealth meet its burden of proof in this case?

> "3. When a judge denies a 'Gelfgatt' motion filed by the Commonwealth and the Commonwealth thereafter renews its motion and provides additional supporting information that it had not provided in support of the motion initially, is a judge acting on the renewed motion first required to find that the additional information was not known or reasonably available to the Commonwealth when the earlier motion was filed before considering the additional information?"

We conclude that when the Commonwealth seeks an order pursuant to our decision in Gelfgatt (Gelfgatt order or motion) compelling a defendant to decrypt an electronic device by entering a password, art. 12 requires the Commonwealth to prove that the defendant knows the password beyond a reasonable doubt for the foregone conclusion exception to apply. We also conclude that the Commonwealth met its burden in this case. Finally, we conclude that a judge acting on a renewed Gelfgatt motion may consider additional information without first finding that it was not known or not reasonably available to the Commonwealth at the time the earlier Gelfgattmotion was filed.

We therefore reverse the judge's denial of the Commonwealth's renewed Gelfgatt motion, and we remand the case to the Superior Court for entry of an order compelling the defendant to enter the password into the cell phone at issue.[2]

Background. The relevant undisputed facts are taken from the parties' submissions to the motion judge.[3] See Gelfgatt, 468 Mass. at 514, 11 N.E.3d 605.

1. The investigation and the defendant's arrest. In December 2016, the police responded to a report of a stolen purse at a hotel in Woburn. Upon arriving, the woman whose purse was stolen, Sara,[4] identified the defendant as the perpetrator of the theft. She explained that she knew the defendant because she had met him through an online dating website a few weeks earlier. Sara eventually disclosed that although she had initially believed that she and the defendant were dating, the defendant soon induced her into working as a prostitute in exchange for housing. Based on this information, the police began investigating the defendant.

During their investigation, police linked a cell phone, later determined to be an LG brand cell phone (LG phone), to the defendant. Sara stated that she communicated with the defendant by contacting the LG phone. Specifically, she "talk[ed] on the phone and [exchanged] text messag[es] with [the defendant]" while he used the LG phone. Additionally, the LG phone's telephone number was listed in the contacts section of Sara's cell phone as "[ ]Dennis."

*3 Sara told police that the LG phone was used by the defendant and a female associate to conduct prostitution. Specifically, Sara explained that the defendant would regularly respond to customer text messages by using the LG phone, but that his female associate would answer telephone calls from customers so that the customers would hear a "female voice." Additionally, an examination of Sara's cell phone revealed several communications between her phone and the LG phone related to prostitution, including screenshots of customer communications sent to the LG phone in response to online advertisements seeking to arrange prostitution transactions with Sara; messages from the LG phone explicitly instructing Sara on how to perform sexual acts on customers; messages from the LG phone trying to convince Sara to return to the defendant after she had attempted to flee from him out of fear; and messages from the LG phone apologizing for the defendant's behavior. Police also discovered several Internet postings on the website Backpage.com advertising Sara as an escort that listed the telephone number of the LG

phone as the principal point of contact for customers seeking to engage in a prostitution transaction with her.

The police arrested the defendant shortly after commencing their investigation. At the time of the arrest, the police recovered two cell phones in his possession, one of which was the LG phone. The LG phone was found in the defendant's pants pocket.

Soon after the arrest, the police applied for a search warrant to perform a forensic search of the LG phone. The application was granted. The police thereafter attempted to execute the search warrant, but discovered that its contents were encrypted such that they could be accessed only after the entry of a password to unlock, and thereby decrypt, the cell phone.[5] The police determined that they did not have the technological capability to bypass the lock function without the entry of the password and were therefore unable to execute the search warrant.

2. The Commonwealth's Gelfgatt motions. As discussed supra, the Commonwealth filed a Gelfgatt motion seeking a court order compelling the defendant to decrypt the LG phone by entering its password. The Commonwealth argued that compelling the defendant to enter the password would not force him to incriminate himself because the act itself would not reveal any information that the Commonwealth did not already know. Following a hearing, a judge denied the motion, concluding that because the Commonwealth had failed to "demonstrate[ ] with reasonable particularity that [the defendant] possesses the [password] for the LG phone," the defendant's knowledge of the password was not a foregone conclusion under the Fifth Amendment.

When the Commonwealth renewed its motion, it presented additional factual information that it argued proved that the defendant's knowledge of the password was a foregone conclusion, including the LG phone's subscriber information that tended to link the defendant to the LG phone, subsets of the LG phone's cell site location information (CSLI) records, and a prior statement the defendant had made to police during his booking in an unrelated criminal matter in which he identified the LG phone as his telephone number. The judge denied the renewed motion.

The Commonwealth filed a petition for relief in the county court, pursuant to G. L. c. 211, § 3. The single justice reserved and reported the case to the full court, asking the parties to address the three questions quoted supra.

*4 [1] Discussion. The Fifth Amendment provides that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." Similarly, art. 12 provides that "[n]o subject shall ... be compelled to accuse, or furnish evidence against himself." Accordingly, it is a "fundamental principle of our system of justice" that a person enjoys the "right to be free from self-incrimination" under the Fifth Amendment and art. 12. Commonwealth v. Borans, 388 Mass. 453, 455, 446 N.E.2d 703 (1983).

[2] [3] [4] [5] The privilege against self-incrimination applies when the "accused is compelled to make a testimonial communication that is incriminating." Fisher v. United States, 425 U.S. 391, 408, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). See Commonwealth v. Burgess, 426 Mass. 206, 218, 688 N.E.2d 439 (1997). Testimonial communications are not limited to spoken words or written statements, however, as the act of producing information "demanded by the government may have 'communicative aspects' that would render the Fifth Amendment" and art. 12 applicable. Gelfgatt, 468 Mass. at 520, 11 N.E.3d 605, quoting Fisher, 425 U.S. at 410, 96 S.Ct. 1569. "Whether an act of production is testimonial depends on whether the government compels the individual to disclose the contents of his [or her] own mind to explicitly or implicitly communicate some statement of fact" (quotations and citation omitted).[6] Gelfgatt, supra at 520, 11 N.E.3d 605. See id. at 525-526, 11 N.E.3d 605 ("Where the information conveyed by an act of production is reflective of the knowledge, understanding, and thoughts of the witness, it is deemed to be testimonial and, therefore, within the purview of art. 12" [quotations and citation omitted]).

[6] The Commonwealth may, however, compel testimonial acts of production without violating a defendant's rights under the Fifth Amendment or art. 12 where the "facts conveyed [by the act] already are known to the government, such that the individual 'adds little or nothing to the sum total of the Government's information.' " Gelfgatt, 468 Mass. at 522, 11 N.E.3d 605, quoting Fisher, 425 U.S. at 411, 96 S.Ct. 1569. In these circumstances, because the facts implicitly disclosed through the act of production are already known to the Commonwealth, they are considered a "foregone conclusion" and do not force a defendant to incriminate himself or herself. Gelfgatt, supra at 522-523, 525-526, 11 N.E.3d 605.

Although the foregone conclusion exception originated in the context of the compelled production of documents in response to a government subpoena, see Fisher, 425 U.S. at 411, 96 S.Ct. 1569, we extended

its application to the compelled production of passwords to encrypted electronic devices in Commonwealth v. Gelfgatt, 468 Mass. at 522-525, 11 N.E.3d 605.[7] In Gelfgatt, the defendant was an attorney who was alleged to have, "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." Id. at 513, 11 N.E.3d 605. The files located on four computers seized from the defendant, however, were encrypted and were thus inaccessible to the Commonwealth without the entry of a password to decrypt them. Id. at 516-517, 11 N.E.3d 605. We concluded that compelling the defendant to decrypt the files by entering the passwords into the computers could be a testimonial act of production under the Fifth Amendment and art. 12. Id. at 522, 525-526, 11 N.E.3d 605. Nonetheless, we held that "[t]he facts that would be conveyed by the defendant through his act of decryption ... already [were] known to the [Commonwealth] and, thus, [were] a 'foregone conclusion.' "[8] Id. at 524, 11 N.E.3d 605. We therefore held that the Commonwealth's motion to compel decryption did not violate either the Fifth Amendment or art. 12. Id. at 524, 525, 11 N.E.3d 605. See id. at 523, 11 N.E.3d 605 (because facts conveyed by act of decryption were foregone conclusion, "the act of decryption is not a testimonial communication that is protected" by Fifth Amendment or art. 12).

*5 [7] Accordingly, for the foregone conclusion exception to apply, the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production. Id. at 522-523, 11 N.E.3d 605. In the context of compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device.[9] See id. See also Kerr, Compelled Decryption and the Privilege Against Self-incrimination, Tex. L. Rev. (forthcoming 2019) (manuscript at 18) ("the only assertion implied by entering the password is that the person compelled knows the password"). The Commonwealth must therefore establish that a defendant knows the password to decrypt an electronic device before his or her knowledge of the password can be deemed a foregone conclusion under the Fifth Amendment or art. 12.[10]

*6 [8] With this analytical framework in mind, we turn now to the reported questions. [11]

*7 1. First reported question: burden of proof in a Gelfgatt motion. The first question reported to us by the single justice is one left unanswered in Gelfgatt: "What is the burden of proof that the Commonwealth bears in [a Gelfgatt motion] in order to establish a foregone conclusion ... ?"

a. Burden of proof under the Fifth Amendment. Although several State and Federal courts have applied the foregone conclusion exception in the context of compelled decryption, apparently only one court has meaningfully articulated the standard of proof the government bears to establish that a defendant's knowledge of the password to decrypt an electronic device is a foregone conclusion under the Fifth Amendment. United States v. Spencer, U.S. Dist. Ct., No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Ca. Apr. 26, 2018). In the Spencer decision, the court concluded that the appropriate standard of proof under the Fifth Amendment is clear and convincing evidence. Id. In so doing, the court explained that this standard places "a high burden on the government to demonstrate that the defendant's ability to decrypt the device at issue is a foregone conclusion." Id. The court noted that a high burden was necessary given the "Fifth Amendment's otherwise jealous protection of the privilege against giving self-incriminating testimony." Id. The Commonwealth argues that this standard of proof should apply to Gelfgatt motions.[12]

[9] The parties have not identified, and we have not found, a United States Supreme Court case -- in Fisher or any subsequent cases -- or any United States Court of Appeals case that has specifically addressed these issues. We need not speculate what the United States Supreme Court would decide is the appropriate standard of proof under the Fifth Amendment, however, as we conclude that art. 12 requires the Commonwealth to prove that a defendant knows the password to decrypt an electronic device beyond a reasonable doubt for the foregone conclusion exception to apply. See Lego v. Twomey, 404 U.S. 477, 489, 92 S.Ct. 619, 30 L.Ed.2d 618 (1972) ("Of course, the States are free, pursuant to their own law, to adopt a higher standard [of proof]. They may indeed differ as to the appropriate resolution of the values they find at stake").

[10] b. Burden of proof under art. 12. The adoption of a standard of proof "represents an attempt to instruct the fact finder concerning the degree of confidence our society thinks he [or she] should have in the correctness of [his or her] factual conclusions.' " Doe, Sex Offender Registry Bd. No. 380316 v. Sex Offender Registry Bd., 473 Mass. 297, 309, 41 N.E.3d 1058 (2015), quoting In re Winship, 397 U.S. 358, 370, 90 S.Ct. 1068, 25 L.Ed.2d 368 (1970) (Harlan, J., concurring). In criminal cases, we require the Commonwealth to prove all essential elements of the crime beyond a reasonable doubt, while generally requiring that other preliminary factual questions related to the admission of evidence be proved only by a preponderance of the evidence. See, e.g., Commonwealth v. Bright, 463 Mass. 421, 432, 974 N.E.2d 1092 (2012) (admission of

out-of-court statements of coventurers); Commonwealth v. Rosenthal, 432 Mass. 124, 126-127 & n.4, 732 N.E.2d 278 (2000) (admission of prior bad acts). We have held, however, that some critical facts implicating a defendant's constitutional rights require proof beyond a reasonable doubt. For example, we have held that the Commonwealth must prove the voluntariness of a defendant's confession beyond a reasonable doubt before the confession may be placed before a jury. Commonwealth v. Tavares, 385 Mass. 140, 152, 430 N.E.2d 1198, cert. denied, 457 U.S. 1137, 102 S.Ct. 2967, 73 L.Ed.2d 1356 (1982). Similarly, in Commonwealth v. Day, 387 Mass. 915, 921, 444 N.E.2d 384 (1983), we held that the Commonwealth must prove that a defendant's waiver of his or her Miranda rights was made knowingly and intelligently beyond a reasonable doubt. In both circumstances, we concluded that the standard of proof beyond a reasonable doubt -- the highest standard considered by courts in their function as fact finders -- was necessary to protect the defendant's rights at issue.

*8 [11] In determining the reach of art. 12's protection of the privilege against self-incrimination, we also are attentive to the difference in wording of art. 12 from the Fifth Amendment. Article 12 protects a defendant from being compelled to "furnish evidence" against himself or herself, as opposed to becoming "a witness against" himself or herself. Based in part on this textual difference, we have "consistently held that art. 12 requires a broader interpretation [of the right against self-incrimination] than that of the Fifth Amendment."[13] Opinion of the Justices, 412 Mass. 1201, 1210, 591 N.E.2d 1073 (1992), quoting Attorney Gen. v. Colleton, 387 Mass. 790, 796, 444 N.E.2d 915 (1982). See Gelfgatt, 468 Mass. at 525, 526, 11 N.E.3d 605(art. 12 "demands a more expansive protection" but nonetheless recognizing the foregone conclusion exception itself and much of its "analytical" structure [citation omitted]); Burgess, 426 Mass. at 218, 688 N.E.2d 439 ("Although 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" [quotations and citation omitted]). Accordingly, this court has remained vigilant to safeguard against governmental conduct that could infringe upon this privilege under art. 12.

With these considerations in mind, we conclude that when the Commonwealth seeks a Gelfgatt order compelling a defendant to decrypt an electronic device by entering a password, art. 12 requires that, for the foregone conclusion to apply, the Commonwealth must prove beyond a reasonable doubt that the defendant knows the password.[14] Whatever the standard under the Fifth Amendment may be, requiring the Commonwealth to bear this high burden is necessary to ensure that the art. 12 rights of defendants are adequately protected, and reflects our recognition that a "person's right to be free from self-incrimination is a fundamental principle of our system of justice," and that we have imposed even higher standards than the Fifth Amendment to protect that right. Borans, 388 Mass. at 455, 446 N.E.2d 703. See Addington v. Texas, 441 U.S. 418, 423, 99 S.Ct. 1804, 60 L.Ed.2d 323 (1979) ("The standard [of proof] serves to allocate the risk of error between the litigants and to indicate the relative importance attached to the ultimate decision"); Commonwealth v. Alicea, 464 Mass. 837, 841–842, 985 N.E.2d 1197 (2013) (under art. 12, witness may not be compelled to testify unless "it is perfectly clear, from a careful consideration of all the circumstances in the case ... that the [testimony] cannot possiblyhave such tendency to incriminate" [citation omitted]). See also Opinion of the Justices, 412 Mass. at 1210, 591 N.E.2d 1073 (discussing broader protections afforded under art. 12).

*9 Most critically, the imposition of this burden is also necessary to respect the meaning and purpose of the foregone conclusion exception. Indeed, as its very name suggests, the government must be certain that the facts conveyed by a compelled act of production are already known before it can properly be considered a foregone conclusion. See Black's Law Dictionary 762 (10th ed. 2014) (defining "foregone conclusion" as "[an] inevitable result; a foreordained eventuality"). The term, as it is used in this legal context, draws its roots from the Supreme Court's decision in Fisher, 425 U.S. at 411, 96 S.Ct. 1569. There, the Court held that the production of tax documents prepared by an accountant was not protected by the Fifth Amendment because the existence and location of the documents were already known to the government and were thus "a foregone conclusion." Id. Their disclosure therefore "add[ed] little or nothing to the sum total of the Government's information." Id. Although in Fisher the Court neither defined the term "foregone conclusion" nor articulated the standard of proof, the Court's discussion suggests that the government must have a high level of certainty that the defendant's act of production will not reveal any factual information beyond what it already knows for the exception to apply. See id. at 410-411, 96 S.Ct. 1569. Indeed, in reaching its conclusion, the Court reasoned that it was "confident" that the disclosure would not violate the Fifth Amendment because "[s]urely the Government [wa]s in no way relyingon the 'truthtelling' of the [defendant] to prove the existence of or his access to the documents" (emphasis added). Id. at 410, 411, 96 S.Ct. 1569.

Our cases addressing the foregone conclusion exception also suggest holding the Commonwealth to a high standard of proof. For example, in Gelfgatt, where the Commonwealth sought to compel the defendant to decrypt several computers, we concluded that the exception applied because the defendant had already admitted to investigators that he had the ability to decrypt the seized computers. Gelfgatt, 468 Mass. at 524, 11 N.E.3d 605. In that circumstance, the Commonwealth conclusively knew that the defendant knew the password, and therefore, his knowledge was a foregone conclusion. Id. By contrast, we concluded in Commonwealth v. Hughes, 380 Mass. 583, 592, 404 N.E.2d 1239, cert. denied, 449 U.S. 900, 101 S.Ct. 269, 66 L.Ed.2d 129 (1980), that the exception did not apply where the Commonwealth sought to compel the defendant to produce a firearm that the Commonwealth suspected had been used in an assault. The defendant was known only to have registered a firearm; he had not reported its sale or transfer, and a search of the defendant's car had not resulted in its discovery. Id. at 584, 585, 404 N.E.2d 1239. We noted that production of the firearm was far from being a "foregone conclusion":

"If the defendant should produce the [firearm], he would be making implicitly a statement about its existence, location and control .... [that] would deal with just those matters about which the Commonwealth desires but does not have solid information.... [T]he Commonwealth is seeking to be relieved of its ignorance or uncertainty by trying to get itself informed of knowledge the defendant possesses" (quotations and citations omitted).

Id. at 592, 404 N.E.2d 1239. Because the production of the firearm would have conveyed facts not already known to the Commonwealth, we did not permit the Commonwealth to compel its production under the Fifth Amendment and art. 12. Id.

[12] These decisions make clear that the Commonwealth must be certain that the compelled act of production will not implicitly convey facts not otherwise known to the Commonwealth. Accordingly, we conclude that the beyond a reasonable doubt standard burdens the Commonwealth with the appropriate level of certainty to prove the fact of a defendant's knowledge of the password to an encrypted electronic device to be a foregone conclusion under art. 12. To require anything less would defeat the meaning and purpose of the exception.

The Commonwealth argues that the privilege against self-incrimination can be adequately protected by the clear and convincing evidence standard. We disagree. Permitting the Commonwealth to prove a defendant's knowledge of the password to an encrypted electronic device by a standard lower than beyond a reasonable doubt creates a greater risk of incorrectly imputing knowledge to those defendants who truly do not know the password. Such an error would bring steep consequences. Indeed, beyond the fact that an error would directly violate the defendant's art. 12 rights, the practical consequence of the erroneous imputation of knowledge would be the issuance of a Gelfgatt order with which the defendant could not possibly comply. The defendant's inevitable failure to comply would likely then lead to a finding of civil or criminal contempt potentially resulting in incarceration. See, e.g., United States v. Apple MacPro Computer, 851 F.3d 238, 247, 249 (3d Cir. 2017), cert. denied sub nom. Doe v. United States, —— U.S. ——, 138 S.Ct. 1988, 201 L.Ed.2d 254 (2018) (reviewing defendant's appeal from contempt order after defendant found in contempt for refusing order to decrypt electronic device). The increased risk of error brought on by a lower standard of proof is not one that we are willing to endorse here.

*10 [13] 2. Second reported question: application to this case. We turn now to the second reported question: whether the Commonwealth met its burden in this case. We conclude that the factual record put before the motion judge by the Commonwealth in its initial Gelfgatt motion and its renewed motion[15] contained sufficient evidence for the Commonwealth to meet its evidentiary burden.

At the start of the investigation of the defendant, Sara made statements to police tending to show the defendant's regular use of the LG phone. Sara stated that she would speak directly with the defendant by calling the LG phone and that she also communicated with him by exchanging text messages with the LG phone. She also explained that the defendant would regularly respond to customer text messages by using the LG phone. Additionally, an examination of Sara's phone revealed that the LG phone's telephone number was listed in the contacts section of her phone as "[ ]Dennis," creating the reasonable inference that, at the very least, Sara understood that the defendant could be reached by contacting the LG phone.[16]

The record also reveals that the LG phone was in the defendant's possession at the time he was arrested by police. Indeed, it was recovered from his front pants pocket. Additionally, the motion judge acknowledged that the record revealed that the defendant had characterized the telephone number of the LG phone as his telephone number to police while he was being booked following an arrest in an unrelated criminal matter approximately one month before he was arrested in this case. Subscriber information for the LG phone also

revealed that the LG phone subscriber had listed a “backup” telephone number. Police records pertaining to this backup telephone number showed that it belonged to a “Dennis Jones” with the same Social Security number and date of birth as the defendant. Finally, the LG phone's CSLI records revealed that at various times, the LG phone was in the same location at the same time as another cell phone that was confirmed to be the defendant's phone. The CSLI records also revealed that the phone calls were made from the LG phone when that phone was confirmed to be miles away from the female associate who assisted the defendant in conducting prostitution (and who had her own personal phone). These facts undoubtedly create the reasonable inference that the defendant regularly used the LG phone and that he therefore knew its password.

The defendant principally argues that his knowledge of the password is not a foregone conclusion because the Commonwealth has failed to prove that he had sole ownership and control of the LG phone. Specifically, the defendant points to evidence in the record showing that the LG phone was used by more than one person and to CSLI records confirming that, at various times, the LG phone and the defendant were in different locations.

*11 Although proof of ownership or exclusive control of the LG phone would certainly further support the Commonwealth's argument, we explained supra that the Commonwealth is only required to establish the defendant's knowledge of the password beyond a reasonable doubt, not his ownership or exclusive control of the LG phone. That multiple people may have used the LG phone and therefore may know its password does not disprove the defendant's knowledge of the password; exclusive control of the phone is not required. This is especially so in light of Sara's characterization of the LG phone as the defendant's business phone that was used by both the defendant and a female associate to arrange and direct prostitution transactions -- a characterization that was corroborated by the record.[17]

The defendant's possession of the phone at the time of his arrest, his prior statement to police characterizing the LG phone's telephone number as his telephone number, the LG phone's subscriber information and CSLI records, and Sara's statements that she communicated with the defendant by contacting the LG phone, taken together with the reasonable inferences drawn therefrom, prove beyond a reasonable doubt that the defendant knows the password to the LG phone. Indeed, short of a direct admission, or an observation of the defendant entering the password himself and seeing the phone unlock, it is hard to imagine more conclusive evidence of the defendant's knowledge of the LG phone's password. The defendant's knowledge of the password is therefore a foregone conclusion and not subject to the protections of the Fifth Amendment and art. 12. The motion judge's denial of the Commonwealth's renewed Gelfgatt motion is therefore reversed.

3. Third reported question: consideration of additional information. The third and final reported question asks us whether a judge may consider additional information included in a renewed Gelfgatt motion only after first finding that the additional information was not known or reasonably available to the Commonwealth at the time the earlier Gelfgatt motion was filed.

[14] We consider first the legal question posed in the reported question. “Upon a showing that substantial justice requires, the judge ... may permit a pretrial motion which has been heard and denied to be renewed.” Mass. R. Crim. P. 13 (a) (5), as appearing in 442 Mass. 1516 (2004). Substantial justice may require consideration of a renewed motion in a number of circumstances, including where the renewed motion contains “new or additional grounds ... which could not reasonably have been known when the motion was originally filed.” Reporters' Notes to Mass. R. Crim. P. 13 (Revised, 2004), Mass. Ann. Laws Court Rules, Rules of Criminal Procedure, at 1597 (LexisNexis 2018). It is well established, however, that the power of a judge to consider a renewed motion “is not restricted to those circumstances” where new facts have been raised. Commonwealth v. Haskell, 438 Mass. 790, 792, 784 N.E.2d 625 (2003). This is particularly true, we conclude, in the context of Gelfgatt motions, which arise in the course of ongoing investigations, often at early stages of such investigations, where the facts are still being investigated and developed.

[15] Accordingly, we answer the third reported question as follows: a judge acting on a renewed Gelfgatt motion may consider additional information without first finding that it was not known or not reasonably available at the time of the first filing.

*12 [16] [17] We turn now to whether the motion judge abused his discretion in this case. See Haskell, 438 Mass. at 792, 784 N.E.2d 625. A judge's decision will be found to be an abuse of discretion only where it contains an error of law or “where we conclude the judge made a clear error of judgment in weighing the factors relevant to the decision, ... such that the decision falls outside the range of reasonable alternatives” (quotations and citation omitted). L.L. v. Commonwealth, 470 Mass. 169, 185 n.27, 20 N.E.3d 930 (2014).

We conclude that the motion judge's decision that he "was not inclined to" consider the additional factual information supporting the Commonwealth's renewed Gelfgatt motion without first finding that it was not known or reasonably available at the time of the first filing was incorrect and based on a mistaken analogy to motions to suppress, where we have imposed tighter constraints on renewed filings. We believe that Gelfgatt motions are more aptly compared to search warrant applications, which can be renewed without similar constraints.

Our conclusion is informed by the particular qualities of a Gelfgatt motion. Much like a search warrant application, a Gelfgatt motion is an investigatory tool that aids investigators in obtaining material and relevant evidence related to a defendant's conduct. Indeed, the purpose of a Gelfgatt motion is to enable the Commonwealth to gain access to an encrypted electronic device, thereby allowing it to further its investigation of a defendant. As a result, one might reasonably expect that some relevant existing facts might be overlooked or missed by investigators when an initial Gelfgatt motion is filed, especially when such a motion is filed early on in an investigation.

[18] [19] We do not consider the judge's apparent analogizing of Gelfgattmotions to motions to suppress to be an apt comparison, as the validity of motions to suppress are based upon the information known at the time of the challenged government conduct. The factual record before the court is therefore a much more fixed target than the one at issue in a Gelfgattmotion; a motion which, as explained supra, is directed at obtaining information necessary for an ongoing investigation, and is informed by that investigation. For example, in reviewing a defendant's motion to suppress that challenges whether there was sufficient probable cause to authorize a search warrant, the reviewing judge is limited to reviewing the four corners of the affidavit in support of a warrant application to determine whether probable cause existed. Commonwealth v. O'Day, 440 Mass. 296, 298, 798 N.E.2d 275 (2003) ("The magistrate considers ... whether the facts presented in the affidavit and the reasonable inferences therefrom constitute probable cause. That conclusion of law is neither buttressed nor diminished by other evidence"). Motions to suppress challenging other evidence must likewise be based on what the police knew at the time of the search. What the police learned later in their investigation is irrelevant to a motion to suppress.[18]

Given the different nature and purpose of a Gelfgatt motion, the motion judge committed an error of law by imposing the tighter constraints required for renewed motions to suppress. The Commonwealth should not have been barred from renewing its initial Gelfgatt motion simply because it failed to ascertain all available facts bearing on a defendant's knowledge of the password to an encrypted device at the time it filed its first Gelfgatt motions. As is allowed for subsequent search warrant applications, the Commonwealth should have been permitted to renew its Gelfgatt motion upon the further development of the factual record of the case. This is especially so in light of our holding today that the Commonwealth must prove the defendant's knowledge of the password beyond a reasonable doubt. This standard of proof is rigorous, and the Commonwealth may use a renewed motion to bring additional factual information that it may have missed in preparing its initial motion to the reviewing court's attention in an attempt to meet this burden. Cf. United States v. Greenfield, 831 F.3d 106, 128 (2d Cir. 2016) (noting, after finding that defendant could not be compelled to produce bank records under foregone conclusion exception, that "we do not ... foreclose the possibility that the Government could develop a better record with respect to each of the relevant requirements in connection with the issuance of another summons in the future. Indeed, it is precisely because of this possibility that we have examined in such detail what is lacking in the present Summons").

*13 [20] This is not to say that courts are required to consider renewed Gelfgatt motions under every circumstance. Incomplete, careless, repetitive, or tardy police or prosecution work need not be tolerated. Decisions concerning whether to consider renewed motions remain in the sound discretion of the motion judge, and will depend on the facts and circumstances of each particular case. A judge may not, however, decline to consider a renewed motion simply because the additional factual information contained in the renewed motion was either known or reasonably available to the Commonwealth at the time the Gelfgatt motion was first filed.

In this case, the renewed filing should have been considered and allowed. Indeed, the Commonwealth had reasonable grounds to believe that its initial motion as filed was sufficient to prove that the defendant's knowledge of the password was a foregone conclusion. The original motion included critical facts bearing on the defendant's knowledge of the password to the LG phone, including the fact that the LG phone was found in his possession at the time of his arrest and the victim's detailed description of the defendant's use of the LG phone. These facts created a strong inference that the defendant knew the LG phone's password. We understand, however, that the novelty of the question and the relative uncertainty of the proper legal standard

in the compelled decryption context made this initial motion difficult for both the judge and the parties. The additional factual information included in the renewed motion, however, certainly resolved any reasonable remaining doubts that may have existed in the initial motion. Although some, if not all, of the additional information included in its renewed motion may very well have been available to the Commonwealth at the time it filed its initial motion, in light of the nature and purpose of Gelfgatt motions and the circumstances of this case, the judge erred in concluding that he need not consider the additional information "[a]bsent a showing of new evidence not otherwise available to the Commonwealth." The motion judge therefore abused his discretion in denying the Commonwealth's renewed Gelfgattmotion.

Conclusion. For the foregoing reasons, the motion judge's denial of the Commonwealth's renewed Gelfgatt motion is reversed, and this case is remanded to the Superior Court for entry of an order compelling the defendant to enter the password into the cell phone at issue.

So ordered.

LENK, J. (concurring).

I write separately because, unlike the court, I think that compelled decryption of a cellular telephone or comparable device implicates more than just its passcode; what the government seeks is access to the files on the device, which the government believes will aid in inculpating the defendant. Given that the foregone conclusion doctrine is a narrow exception to the constitutional privilege against self-incrimination, the government may compel a defendant's decryption of such a device only when it can show that any testimonial aspect involved in that act of production is already known to the government. In other words, the government must demonstrate, beyond a reasonable doubt, that the accused knows the passcode to the device and that the government already knows, with reasonable particularity, the existence and location of relevant, incriminating evidence it expects to find on that device. Because here the government met these requirements, I concur in the result. I also agree with the court that the appropriate standard of proof is beyond a reasonable doubt, and that the judge should have allowed the Commonwealth to present new evidence in an additional motion to compel.

*14 Act of producing files. "A person's right to be free from self-incrimination is a fundamental principle of our system of justice," secured both by art. 12 of the Massachusetts Declaration of Rights and the Fifth Amendment to the United States Constitution. See Commonwealth v. Borans, 388 Mass. 453, 455, 446 N.E.2d 703 (1983). The constitutional privilege, however, applies only when an accused is "compelled to make a testimonial communication that is incriminating" (emphasis omitted). See Fisher v. United States, 425 U.S. 391, 408, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). The United States Supreme Court has long held that, in some instances, the act of producing evidence can be an incriminating, testimonial communication because an accused "tacitly concedes" the existence, custody, and authenticity of the evidence. See Fisher, supra at 410, 96 S.Ct. 1569. When such is the case, the Fifth Amendment privilege against self-incrimination is implicated. Id.

The "foregone conclusion" doctrine, first articulated by the United States Supreme Court in Fisher, and relied upon in Commonwealth v. Gelfgatt, 468 Mass. 512, 526, 11 N.E.3d 605 (2014), provides a narrow exception to the otherwise uncompromising privilege against self-incrimination. Under the Fifth Amendment and art. 12, the exception applies only where any testimonial aspects inherent in the act of producing evidence are a "foregone conclusion" already known to the government. See Fisher, 425 U.S. at 411, 96 S.Ct. 1569; Gelfgatt, supra. That is, where the government demonstrates its prior knowledge of the "existence and location of the papers" it seeks to compel, the accused "adds little or nothing to the sum total of the Government's information by conceding that he [or she] in fact has the papers." Fisher, supra at 411, 96 S.Ct. 1569. Under such circumstances, an accused's Fifth Amendment privilege is not implicated, as "[t]he question is not of testimony but of surrender." Id. at 411, 96 S.Ct. 1569.

Compelled decryption. Although these Fifth Amendment doctrines find their provenance in cases involving subpoenaed paper documents, courts since have applied their underlying principles to electronic documents in the context of compelled decryption. See, e.g., United States v. Apple MacPro Computer, 851 F.3d 238, 247 (3d Cir. 2017), cert. denied sub nom. Doe v. United States, —— U.S. ——, 138 S.Ct. 1988, 201 L.Ed.2d 254 (2018); In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1342 (11th Cir. 2012) (In re Grand Jury Subpoena); In re Boucher, U.S. Dist. Ct., No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). Indeed, in Gelfgatt, we held that, for the foregone conclusion exception to apply to an order compelling decryption of a device, "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 Gelfgatt, 468 Mass. at 522, 11 N.E.3d 605, citing Fisher, 425 U.S. at 410-413, 96 S.Ct. 1569; United States v. Bright, 596 F.3d 683, 692 (9th Cir. 2010); and United States v. Hubbell, 530 U.S. 27, 40-41, 44-45, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000). That is, by entering a passcode to provide the government with unencrypted access to a device, "the defendant implicitly would be acknowledging that he has ownership and control of the [devices] and their contents." See Gelfgatt, supra at 522, 11 N.E.3d 605. Unless the government demonstrates that such information already is a foregone conclusion, the Fifth Amendment protection bars it from compelling an accused to provide it. See id. at 522-523, 11 N.E.3d 605.

For the foregone conclusion exception to apply, the government also "must be able to 'describe with reasonable particularity' the documents or evidence it seeks to compel." Apple MacPro Computer, 851 F.3d at 247, quoting Hubbell, 530 U.S. at 29-30, 120 S.Ct. 2037. Although the government is not required to name every document it seeks or what its contents contain, it must demonstrate, with reasonable particularity, the existence and location of some incriminating files it expects to find on the device. See, e.g., Matter of the Decryption of a Seized Data Storage Sys., U.S. Dist. Ct., No. 13-M-449, 2013 WL 12327372 (E.D. Wis. Apr. 19, 2013)(government must demonstrate its "knowledge of the existence, possession, and authenticity of the files on the encrypted storage devices with reasonable particularity"); 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 kn[ew] of existence and location of the computer's files," although not specific content of documents, and knew of defendant's custody and control of device).[1]

*15 Indeed, those United States Courts of Appeals that have addressed these issues in the context of compelled decryption have recognized that the foregone conclusion doctrine requires a showing, with reasonable particularity, as to the existence and location of incriminating files on a device.[2] See, e.g., In re Grand Jury Subpoena, 670 F.3d at 1346 (applying reasonable particularity in context of compelled decryption); Apple MacPro Computer, 851 F.3d at 247 (same). See also Matter of M.W., Ohio Ct. App., No. 2018CA0021, 2018 WL 6787946 (Dec. 21, 2018) (same). For example, In re Grand Jury Subpoena, supra, involved the lawful taking of an accused's digital devices pursuant to a search warrant; a subpoena duces tecum subsequently issued to compel the accused to unlock the devices because law enforcement could not do so. Id. at 1139. There, the court held that, before the government could compel an accused to unlock the device and produce access to the files contained therein, the government had to demonstrate, with reasonable particularity, its awareness that incriminating files exist and are located on those devices, and that the defendant has the ability to unlock and produce them. Id. at 1349.[3] And if this is what the Fifth Amendment requires, well, art. 12 demands even more. See Gelfgatt, 468 Mass. at 525, 11 N.E.3d 605, quoting Commonwealth v. Burgess, 426 Mass. 206, 218, 688 N.E.2d 439 (1997) (we have consistently held that art. 12 provides broader "protection against self-incrimination than does the Fifth Amendment" and provides greater protection). In fact, art. 12 provides that no subject shall be compelled to "furnish evidence against himself" (emphasis added). See Matter of a Grand Jury Investigation, 92 Mass. App. Ct. 531, 534, 88 N.E.3d 1178 (2017), citing Gelfgatt, supra at 523, 11 N.E.3d 605 (Commonwealth need not establish knowledge of specific contents of device, but is required "to demonstrate knowledge of the existence and the location of the content"). The court's departure from this constitutional doctrine is thus, in my view, imprudent, particularly in light of the vast amount of potentially incriminating information at risk.[4]

Because the Commonwealth here has demonstrated its prior knowledge of the existence and location of specific files contained on the LG telephone, however, I conclude that it has met its burdens. More specifically, the government made plain its knowledge of (1) specific text messages, sent from the LG telephone, related to illegal, commercial sex acts; (2) several online advertisements for commercial sex services that featured the woman's image, posted by the LG telephone, on specified dates; (3) particular text messages sent to the alleged victim from the LG telephone; (4) precise dates for CSLI location information for the LG telephone that corresponded to the location of the defendant and the locations where some of the sex services were provided; (5) distinct "screenshot" photographs of conversations with clients from the LG telephone; and (6) records of a hotel reservation, where the defendant was arrested, using the LG telephone's number and the defendant's electronic mail address. Such a comprehensive showing of the government's prior knowledge of these particularized files on the LG telephone compels the conclusion that the Commonwealth has met its burden in this instance.

*16 Conclusion. The court's decision today sounds the death knell for a constitutional protection against compelled self-incrimination in the digital age. After today's decision, before the government may order an individual to provide it with unencrypted access to a trove of potential incriminating and highly personal data on an electronic device, all that the government must demonstrate is that the accused knows the device's passcode. This is not a difficult endeavor, and in my judgment, the Fifth Amendment and art. 12 demand

more. That is, before the government may compel an accused's assistance in building a case against that accused, the government must demonstrate that it already knows, with reasonable particularity, of files on the device relevant to the offenses charged, and that the defendant knows the passcode to unlock them. Because I conclude that the government here met those burdens, I join in the court's result.

[1]

We understand the word “password” to be synonymous with other terms that cell phone users may be familiar with, such as Personal Identification Number or “passcode.” Each term refers to the personalized combination of letters or digits that, when manually entered by the user, “unlocks” a cell phone. For simplicity, we use “password” throughout. See generally, Kerr & Schneier, Encryption Workarounds, 106 Geo. L.J. 989, 990, 994, 998 (2018).

[2]

We acknowledge the amicus briefs submitted by the Attorney General of the Commonwealth of Massachusetts, the Committee for Public Counsel Services, and Professor Orin S. Kerr. We also acknowledge the amicus submission of Professor Laurent Sacharoff.

[3]

These submissions included the Commonwealth's initial search warrant application, and exhibits attached thereto; various affidavits of law enforcement officers, and exhibits attached thereto. The motion judge did not hear testimony from any witnesses or make any credibility findings. He denied the motion based on the documentary record.

[4]

A pseudonym. See G. L. c. 265 § 24C .

[5]

We recognize that ordinary cell phone users are likely unfamiliar with the complexities of encryption technology. For instance, although entering a password “unlocks” a cell phone, the password itself is not the “encryption key” that decrypts the cell phone's contents. See Kerr & Schneier, supra at 995. Rather, “entering the [password] decrypts the [encryption] key, enabling the key to be processed and unlocking the phone. This two-stage process is invisible to the casual user.” Id. Because the technical details of encryption technology do not play a role in our analysis, they are not worth belaboring. Accordingly, we treat the entry of a password as effectively decrypting the contents of a cell phone. For a more detailed discussion of encryption technology, see generally Kerr & Schneier, supra.

[6]

For example, the privilege against self-incrimination is not implicated when the government seeks “to compel an individual to be the source of real or physical evidence by, for example,” furnishing a blood sample, taking a breathalyzer test, producing a voice exemplar, providing a handwriting exemplar, standing in a lineup, or putting on particular clothing. Commonwealth v. Gelfgatt, 468 Mass. 512, 521, 11 N.E.3d 605 (2014) , and cases cited. In these circumstances, the conduct is not testimonial because the “the individual is not required to disclose any knowledge he [or she] might have or to speak his [or her] guilt” (quotations and citation omitted). Id. at 521, 11 N.E.3d 605 .

[7]

Several other courts have done the same. See, e.g., United States v. Apple MacPro Computer, 851 F.3d 238, 247-248 (3d Cir. 2017), cert. denied sub nom. Doe v. United States, —— U.S. ——, 138 S.Ct. 1988, 201 L.Ed.2d 254 (2018); In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344-1345 (11th Cir. 2012) (Subpoena Duces Tecum); United States v. Spencer, U.S. Dist. Ct., No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Ca. Apr. 26, 2018); State v. Stahl, 206 So.3d 124, 135-137 (Fla. Dist. Ct. App. 2016).

[8]

In Gelfgatt, we noted that by entering the passwords, the defendant implicitly conveyed the fact that he knew the computers were encrypted, that he knew the passwords to decrypt the computers, and that he had “ownership and control of the computers and their contents.” Gelfgatt, 468 Mass. at 524, 11 N.E.3d 605 .

Although correctly describing the facts in Gelfgatt, we clarify today that the entry of a password alone does not convey the fact of "ownership" of the device or its contents. Id. Whether entry of a password indicates control also is unclear. Indeed, individuals may very well know the password to an electronic device that is owned and controlled by another person. For example, family members and significant others routinely know the passwords to each other's cell phones, and students are regularly given passwords to school-owned computers. The fact of knowledge of a password is distinct from the ownership or control of the device and its contents.

[9]

The Commonwealth's Gelfgatt motions in this case requested that the defendant "produce" or "provide" the password to the LG phone. Although it is not perfectly clear what the Commonwealth meant by "produce" or "provide," its proposed order suggested that it sought to require the defendant to make a written disclosure of the actual password to the LG phone. There is some debate among courts and commenters as to whether the foregone conclusion exception can apply in cases where the government seeks to compel the defendant to disclose -- whether orally or in writing -- the actual password, as opposed to cases requiring merely physically entering it into the device. Compare Stahl, 206 So.3d at 134 (password itself has no "testimonial significance" and thus may be compelled [citation omitted]), with Spencer, U.S. Dist. Ct., No. 17-cr-00259-CRB-1("the government could not compel Spencer to state the password itself, whether orally or in writing"), and Sacharoff, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203, 236 (2018) ("It is a mistake to apply the foregone conclusion doctrine to the oral disclosure of a password"). See generally Doe v. United States, 487 U.S. 201, 210 n.9, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988) (compelling someone to reveal combination to wall safe, as opposed to merely surrender key to strong box, is testimonial). There is some support for the idea that the written disclosure of the password would amount to direct testimony, not an act of production, and that the foregone conclusion exception is limited only to acts of production. 3 W.R. LaFave, J.H. Israel, N.J. King, & O.S. Kerr, Criminal Procedure § 8.13(a) (4th ed. 2015)("requir[ing a] party to reveal a pass[word] that would allow [the government] to perform the decryption ... would require a testimonial communication standing apart from the act of production, and therefore make unavailable the foregone conclusion doctrine"). We need not, and do not, resolve this distinction here, and our decision is therefore limited to only the physical entry of the password by the defendant, as we required in Gelfgatt. The defendant may therefore only be compelled to enter the password to the LG phone, not disclose it.

[10]

The motion judge interpreted our decision in Gelfgatt to require that the Commonwealth establish "(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." What the motion judge meant by evidence in this context is not particularly clear, nor were we as clear as we might have been in our analysis in Gelfgatt. We clarify that the evidence at issue in the compelled decryption here is the password itself, not the contents of the phone.

As we explained supra, the only testimony that would be conveyed by compelling the defendant to enter the password is the fact that the defendant knows the password, and therefore has the ability to access the phone. The entry would convey no information about the contents of the LG phone. See Stahl, 206 So.3d at 136 ("The question is not the State's knowledge of the contents of the phone; the State has not requested the contents of the phone"). The analysis would be different had the Commonwealth sought to compel the defendant to produce specific files located in the contents of the LG phone. If that had been the case, the production of the files would implicitly convey far more information than just the fact that the defendant knows the password. See Subpoena Duces Tecum, 670 F.3d at 1347, 1349 . The defendant's production of specific files would implicitly testify to the existence of the files, his control over them, and their authenticity. United States v. Hubbell, 530 U.S. 27, 36 n.19, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) ("by producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic"). Accordingly, the Commonwealth would be required to prove its prior knowledge of those facts.

[11]

The concurrence suggests that in addition to proving the defendant's knowledge of the password, the government must also demonstrate that it "already knows, with reasonable particularity, the existence and location of relevant, incriminating evidence it expects to find on that device." Post at ——, —— N.E.3d ——. Without this added requirement, the concurrence argues, the government may obtain "unlimited ... access," postat ——, —— N.E.3d —— note 4, to a "trove of potential incriminating and highly personal data

on an electronic device" by proving only "that the accused knows the device's pass[word]," post at ——, —— N.E.3d ——. This is not correct.

It is well established that under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, the police are ordinarily required to obtain a search warrant before a search of the contents of an electronic device may take place. See, e.g., Riley v. California, 573 U.S. 373, 386, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014) (cell phones); Commonwealth v. Mauricio, 477 Mass. 588, 594, 80 N.E.3d 318 (2017) (digital cameras); Commonwealth v. McDermott, 448 Mass. 750, 776, 864 N.E.2d 471, cert. denied, 552 U.S. 910, 128 S.Ct. 257, 169 L.Ed.2d 188 (2007) (computers). Accordingly, in this case, the police were required to obtain a warrant before they could seek to search the contents of the LG phone, and they did so. The full protections against improper searches -- probable cause to believe that a crime had been committed and that evidence of the crime would be found on the device -- were required and, in the opinion of the clerk-magistrate who issued the search warrant, were satisfied here. The standard proposed by the concurrence conflates these protections with the protections afforded by art. 12 of the Massachusetts Declaration of Rights. Our task under art. 12 in this context is to determine only what facts are conveyed to the government when a defendant is compelled to enter a password to decrypt an electronic device. As we have explained, the only fact conveyed by the physical act of entering the password into an electronic device is that the defendant knows the password. Such an act says nothing about the contents of the device. Nor does the act alone "produce" any evidence to the Commonwealth. Post at ——, —— N.E.3d —— note 1.

Accordingly, under these circumstances, the Commonwealth was required to abide by two sets of constitutional protections. Requiring this dual protection does not, as the concurrence contends, sound a "death knell" of constitutional protection in the digital age. Post at ——, —— N.E.3d ——. Nor do we read the two constitutional protections in "splendid isolation." Post at note 1. Each has its own purpose, function, and requirements, and they work together to form a double protection of digital privacy before particular files on the phone can be accessed.

Moreover, cases from the United States Courts of Appeals cited by the concurrence in support of its proposed standard do not support its application to cases where, as here, the government seeks only to compel the entry of the password to an electronic device. Post at ——, —— N.E.3d ——. For example, the Eleventh Circuit's decision in Subpoena Duces Tecum was a case where the government "served [the defendant] with a subpoena duces tecum requiring him to ... produce the unencrypted contents located on the hard drives of ... laptop computers and five external hard drives" (emphasis added). Subpoena Duces Tecum, 670 F.3d at 1337. There, the government sought not only to compel the defendant to enter the passwords to the devices, but also to compel the defendant to identify and produce the files located in the device in their unencrypted state. Id. The compelled act of identifying and producing files conveys far more information to the government than what the Commonwealth seeks in this case. See note 10, supra. The reference by the concurrence to the Third Circuit's decision in Apple MacPro Computer is similarly unavailing. As the concurrence acknowledges, although the Third Circuit did apply the concurrence's proposed standard in that case, it did so while reviewing the Federal District Court's application of the standard for plain error and expressly stated that "[i]t is important to note that we are not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the 'foregone conclusion' inquiry in the context of a compelled decryption order" (emphasis added). Apple MacPro Computer, 851 F.3d at 248 n.7. The court went on to note that "a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is 'I, [the defendant], know the password for these devices.' " Id.

[12]

Professor Orin Kerr, as amicus curiae, argues in favor of imposing the clear and convincing evidence standard under the Fifth Amendment as well, advocating that the standard is both "consistent with the Supreme Court decision" in Fisher "that established the foregone conclusion doctrine," and "a fair approximation of [the] burden needed to eliminate" the prosecutorial advantage that can be obtained from compelling testimonial acts of production. He takes no position, however, on the appropriate standard under art. 12.

[13]

Indeed, the Fifth Amendment requires the voluntariness of a confession and the waiver of Miranda rights to be proved only by a preponderance of the evidence. See Colorado v. Connelly, 479 U.S. 157, 168-169, 107 S.Ct. 515, 93 L.Ed.2d 473 (1986).

[14]

The motion judge required the Commonwealth to prove the defendant's knowledge of the password, and the existence of information relevant to the charges against the defendant within the LG phone, with "reasonable particularity." This standard has been used to define the level of particularity required in the identification of subpoenaed documents. See, e.g., Subpoena Duces Tecum, 670 F.3d at 1349 ("We find no support in the record for the conclusion that the Government, at the time it sought to compel production [of the subpoenaed electronic files], knew to any degree of particularity what, if anything, was hidden behind the encrypted wall"). Here, neither documents nor the contents of the LG phone are sought. As we explained supra, the Commonwealth therefore need not prove any facts with respect to the contents of the LG Phone. The only consideration is whether the defendant knows the password to the encrypted device. The reasonable particularity standard, which considers the level of specificity with which the Commonwealth must describe sought after evidence, is therefore inapt in the context of compelled decryption. Indeed, as other courts have noted, the defendant either knows the password or does not. His knowledge therefore must be proved to a level of certainty, not described with a level of specificity. See Spencer, U.S. Dist. Ct., No. 17-cr-00259-CRB-1 ("While physical evidence may be described with more or less specificity ... a defendant's ability to decrypt is not subject to the same sliding scale. He [or she] is either able to do so, or he [or she] is not. Accordingly, the reasonable particularity standard cannot apply to a defendant's ability to decrypt a device"). We need not address how the reasonable particularity standard combines with the proof beyond a reasonable doubt requirement in document production cases, as no such content has been sought in this case.

[15]

The additional information included in the renewed motion should have been considered by the motion judge. See part 3, infra. We therefore consider it in evaluating whether the Commonwealth met its burden.

[16]

The motion judge, without explanation, appears to have declined to consider Sara's statements related to the connection between the defendant and the LG phone, concluding that he could not "put much stock in the statements of the complaining witness."

[17]

The record revealed several communications between Sara's phone and the LG phone related to prostitution, including screenshots of customer communications in response to online advertisements for prostitutions transactions with Sara; messages from the LG phone explicitly instructing Sara on how to perform sexual acts on customers; and several Internet postings on the website Backpage.com advertising Sara as an escort and listing the LG phone's telephone number as the principal point of contact.

[18]

We recognize that a defendant may learn through discovery more about what the police knew at the time of the search, thereby justifying a renewed motion to suppress, but this is still a more fixed, time defined inquiry than one connected to an ongoing criminal investigation.

[1]

The Fourth and Fifth Amendments to the United States Constitution and their relationship to each other in the criminal context have long been understood in different ways by judges and legal scholars. See generally Sacharoff, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203, 246-247 (2018). See also Carpenter v. United States, —— U.S. ——, 138 S.Ct. 2206, 2271, 201 L.Ed.2d 507 (2018)(Gorsuch, J., dissenting) (noting that "there is substantial evidence that the [Fifth Amendment's] privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence" [citations omitted]). It is not surprising, then, that the court and I would have different views on these much debated issues. This is especially so as we are called upon to meet the challenges emerging from encrypted devices seized by the government with a valid search warrant, which devices the government seeks to compel an individual to decrypt. My view is that the coequal amendments do not dwell in splendid isolation, and that the Fourth Amendment does not somehow limit or trump the Fifth Amendment whenever there may be a valid search warrant. As a result, it will no longer do to cower in the presence of a search warrant, but to attempt to reconcile the Fourth Amendment's authorization of the government's taking of evidence with the Fifth Amendment's limitations on its requiring an individual to produce it. See Sacharoff, supra at 208 (suggesting rule that "a court may compel a suspect to decrypt only those files that (1) the government already knows the person possesses, and (2) the government can

describe with reasonably particularity. Once the government has identified the specific files, it may compel the defendant to decrypt only those files."). Other courts have adopted or applied rules that may be seen as effecting something of a reconciliation. See e.g., In re Grand Jury Subpoena, 670 F.3d at 1344 ; Apple MacPro Computer, 851 F.3d at 247-248; Matter of the Decryption of a Seized Data Storage Sys., U.S. Dist. Ct., slip op. Contrast United States v. Spencer, U.S. Dist. Ct., No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Ca. Apr. 26, 2018). In any event, what is before us is not the propriety of the rather broad search warrant here, but the constraints imposed by the Fifth Amendment. My reading of what the cases require recognizes those constraints and gives them meaningful teeth.

[2]

As discussed, I do not contend that the contents of the files contained on the phone are protected by the Fifth Amendment, or are the focus of the foregone conclusion inquiry in the context of the compelled decryption of the device itself.

[3]

Likewise, Apple MacPro Computer, 851 F.3d at 241 , concerned the government's "ability to compel the decryption of digital devices when the government seizes those devices pursuant to a valid search warrant." There, the court noted that "the Government has provided evidence to show both [1] that files exist on the encrypted portions of the devices and [2] that [the accused] can access them." Id. at 248. Because the government demonstrated those two things, the court concluded that the magistrate judge did not err in determining "that any testimonial component would be a foregone conclusion." Id. Although the court applied the foregone conclusion and reasonable particularity doctrines to those facts, it also acknowledged that it "need not decide ... that the inquiry can be limited to the question of whether [the accused's] knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine," but that a sound argument could be made in support of such a position. See id. at 248 n.7.

[4]

Permitting the government to undertake a "quintessential fishing expedition" by ordering an individual to enter a passcode and to provide the government with unlimited, unencrypted access to a personal electronic device is precisely the sort of act against which the Fifth Amendment was designed to guard. See United States v. Hubbell, 530 U.S. at 32, 34 n.8, 120 S.Ct. 2037, quoting United States v. Hubbell, 11 F.Supp.2d 25, 37 (D. D.C. 1998) (privilege against self-incrimination, in part, was structured to prevent government from "uncover[ing] uncharged offenses"). See generally Sacharoff, supra at 246-247.

End of Document.