# Unlocking Your Phone Could Lock You Up: Say Your Goodbyes to the Right Against Self-Incrimination

*Cambrea Beller*[*]

## INTRODUCTION

As the U.S. legal system is struggling to adapt to the digital world,[1] more and more Americans own and use electronic devices.[2] Today, ninety-six percent of American adults own cell phones, with individuals looking at their phones an average of fifty-two times per day.[3] The cell phone is an omnipresent device with the ability to carry "millions of pages of text, thousands of pictures, or hundreds of videos" inside a person's pocket.[4] Despite an increased preference to use cell phones to manage daily activities, eighty-three percent of American citizens are "very" or "fairly" concerned about the storage of their personal data.[5] This concern is well-founded as the contents of electronic devices are not afforded adequate protection under the U.S. Constitution.[6]

The disconnect between the law and the digital world is demonstrated by the failure of the courts to satisfactorily apply the Fifth Amendment right

[*] J.D., *cum laude*, New England Law | Boston (2021). B.S., Political Science, Weber State University (2018).

[1] *See, e.g.*, Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-To-Arrest Exception to the Cell Phone as "Hybrid,"* 60 DRAKE L. REV. 429, 440–41 (2012) (discussing the disconnect between the law and technology as it relates to search warrants and cell phones).

[2] *See Mobile Fact Sheet*, PEW RES. CENTER (Apr. 7, 2021), https://perma.cc/9CKY-XNHP .

[3] *Id.*; *2018 Global Mobile Consumer Survey: US Edition*, DELOITTE 3, https://perma.cc/MAU3-96ZY (last visited Oct. 16, 2021) (discussing cell phone use by Americans, with around ninety percent or more of eighteen to fifty-four year olds owning a cell phone).

[4] Riley v. California, 573 U.S. 373, 375 (2014).

[5] *2018 Global Mobile Consumer Survey: US Edition*, *supra* note 3, at 8.

[6] *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 769 (2019) ("Courts have disagreed on the correct answer, as have scholars, with both offering a range of standards for how the Fifth Amendment privilege should apply.").

against self-incrimination as it pertains to warranted searches of a defendant's electronic device.[7] The immense storage capacity of electronic devices, particularly smartphones, intensifies the need to protect the contents on the device.[8] For example, an Apple iPhone can store more than 512 gigabytes of data, depending on the model.[9] This is equivalent to millions of pages of personal information "about who we are, what we know, and what we have done."[10] Phones are no longer just a means of communication; they create a digital footprint that details nearly every aspect of an individual's life.[11]

To search an electronic device without violating the Fourth Amendment, the government is required to obtain a search warrant.[12] But what happens when the government is unable to execute a search warrant because the device is encrypted?[13] Do we force a defendant who has raised a Fifth Amendment right against self-incrimination to assist the government's case by unlocking the device?[14] While the authors of the Constitution and the Bill of Rights could never imagine today's convenient world of technology, it does not stand to reason that the information found on an electronic device is any less worthy of constitutional protection than physical documents.[15] If

---

[7] *See* Kerr, *supra* note 6. *Compare* United States v. Apple MacPro Comput., 851 F.3d 238, 247 (3d Cir. 2017) (holding that the privilege against self-incrimination does not apply if the government can describe the incriminating files that are on the device with reasonable particularity), *with* State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) (holding that the privilege against self-incrimination does not apply when the government can show the defendant has the ability to unlock the device).

[8] *See Riley*, 573 U.S. at 393 (concluding that the storage capacity of cell phones "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse").

[9] *Compare iPhone Models*, APPLE, https://perma.cc/4A4V-DA2D (last visited Oct 16, 2021) (showing the storage capacity of iPhones ranges from 16 gigabytes for the iPhone 6 to up to 1 terabyte (equivalent to 1024 gigabytes) for the newest models).

[10] Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404–05 (2013).

[11] *See generally* Kerr, *supra* note 10, at 405.

[12] *See* U.S. CONST. amend. IV (recognizing the right to be protected against unreasonable searches and seizures, unless the government gets a search warrant based on probable cause that particularly describes the place to be searched, and the persons or things to be seized); *Riley*, 573 U.S. at 403.

[13] *See, e.g.*, Commonwealth v. Jones, 481 Mass. 540, 541 (2019) ("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.").

[14] *See, e.g.*, *id.* at 561 (compelling the defendant who raised the Fifth Amendment privilege to enter the password into the cell phone at issue).

[15] *See generally id.*

anything, the capability of electronic devices to store vast quantities of information points to a greater need for legal protection.[16]

This Comment illustrates that the Supreme Judicial Court ("SJC") failed to follow precedent in *Commonwealth v. Jones* by incorrectly concluding that the only fact conveyed by compelling a defendant to unlock an electronic device is that the defendant knows the password to the device. This Comment further argues that this conclusion violates an individual's Fifth Amendment right against self-incrimination. Part I of this Comment details the right against self-incrimination as a fundamental right under the U.S. Constitution. Part II discusses *Commonwealth v. Jones*, focusing on the analytic framework created by the SJC. Part III argues that the knowledge of the password is not the only testimony conveyed by entering the password to an electronic device. Part IV proposes a new standard to compel a defendant to decrypt an electronic device without violating the Fifth Amendment.

## I. Background

### A. *The Right Against Self-Incrimination Guaranteed to Citizens of Massachusetts*

The Massachusetts Constitution guarantees the right against self-incrimination in Article 12 of the Declaration of Rights.[17] This right derives further protection under Massachusetts case law (as outlined by the Massachusetts Guide to Evidence),[18] and, most importantly, under the Fifth Amendment of the U.S. Constitution.[19] To properly assert the right against self-incrimination under the U.S. Constitution, an individual compelled to testify or produce evidence must be subject to criminal liability,[20] the evidence must have a testimonial aspect, and the state must compel the production.[21]

### B. *An Exception to the Right Against Self-Incrimination*

The *Massachusetts Guide to Evidence* lists six exceptions to a defendant's right against self-incrimination.[22] The exception of most relevance here is the

---

[16] *See Riley*, 573 U.S. at 398 (discussing how the privacy interests of electronic devices "dwarf" those in physical form).

[17] MASS. CONST. art. XII.

[18] SJC ADVISORY COMM. ON MASS. EVIDENCE LAW, MASSACHUSETTS GUIDE TO EVIDENCE § 511 (2021), https://perma.cc/3GVC-59CR [hereinafter MASS. GUIDE TO EVID.]

[19] U.S. CONST. amend. V.

[20] *See* In re Enforcement of Subpoena, 435 Mass. 1, 1–3 (2001).

[21] Commonwealth v. Conkey, 430 Mass. 139, 142–43 (1999).

[22] MASS. GUIDE TO EVID., *supra* note 18, § 511(c).

"foregone conclusion" doctrine.[23] The "foregone conclusion" doctrine deems that "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."[24] Simply put, if the government can demonstrate it had knowledge of the compelled testimony, that testimony is not protected by the Fifth Amendment.[25]

The U.S. Supreme Court introduced the "foregone conclusion" exception in *Fisher v. United States*.[26] The defendants in *Fisher* invoked their Fifth Amendment right against self-incrimination after the government compelled them to produce certain tax return documents.[27] The Court reasoned that, by producing evidence in compliance with a subpoena, the defendants implicitly acknowledged the existence and control of the compelled documents.[28]

The Court concluded that the tax documents were not protected by the Fifth Amendment because the government demonstrated it already knew of the existence and location of these tax documents.[29] The Court explained that the government was "in no way relying on the 'truth-telling' of the [defendant] to prove the existence of or his access to the documents."[30] Compelled production would not contribute to the sum total of the government's information; thus, the government sufficiently demonstrated that the existence and location of the papers were a "foregone conclusion."[31] The Court further stated that "however incriminating the contents . . . might be, the act of producing them the only thing which the [defendant] is compelled to dowould not itself involve testimonial self-incrimination."[32] Consequently, the "foregone conclusion" doctrine allows the government to compel the production of incriminating testimony without violating the Fifth Amendment.[33]

---

[23] MASS. GUIDE TO EVID., *supra* note 18, § 511(c)(6).

[24] Commonwealth v. Gelfgatt, 468 Mass. 512, 531 (2014) (Lenk, J., dissenting).

[25] *Id.*

[26] 425 U.S. 391, 410–11 (1976).

[27] *Id.* at 395.

[28] *Id.* at 410.

[29] *Id.* at 411.

[30] *Id.*

[31] *Id.*at 410.

[32] *Fisher*, 425 U.S. at 410–11.

[33] Jesse Coulon, Comment, *Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in* State v. Stahl, 59 B.C. L. REV. E.-SUPPLEMENT 225, 233 (2018).

### C. *The Compelled Decryption of an Electronic Device May Be Considered Testimonial Communication*

While the "foregone conclusion" exception originated in the context of the compelled production of documents,[34] the SJC expanded its application to the compelled production of passwords to encrypted electronic devices in *Commonwealth v. Gelfgatt*.[35] The SJC found that the "factual statements that would be conveyed by entering an encryption key in the computers are 'foregone conclusions,'" and therefore held that "decryption is not a testimonial communication that is protected by the Fifth Amendment"; thus, the Court did not permit a self-incrimination privilege for the compelled decryption of electronic devices.[36]

The defendant in *Gelfgatt* was arrested for orchestrating a fraudulent mortgage scheme, ultimately scamming people out of more than $13 million.[37] The police obtained four of the defendant's computers, and the Commonwealth filed a motion to compel the defendant to decrypt the computers by entering a password.[38] The defendant later refused to comply with the motion, claiming that compliance would force the defendant to incriminate himself.[39]

The Commonwealth asserted that the computers were "virtually impossible to circumvent"—therefore, the motion was necessary to discover material evidence relating to the defendant's purported mortgage scheme.[40] The Commonwealth further raised a "foregone conclusion" argument, contending that "decryption would not communicate facts of a testimonial nature to the [government] beyond what the defendant already had admitted to investigators."[41] The *Gelfgatt* Court concluded that the defendant would implicitly be acknowledging ownership and control of the computers and their contents by decrypting the four computers seized by the Commonwealth;[42] thus, the defendant's compelled act of decryption appeared to be testimonial communication afforded protection under the Fifth Amendment.[43]

---

[34] *See Fisher*, 425 U.S. at 391.

[35] 468 Mass. 512, 512 (2014).

[36] *Id.* at 523.

[37] *Id.* at 515.

[38] *Id.* at 516-17. *See generally* Commonwealth v. Jones, 481 Mass. 540, 542 (2019) (defining a motion to compel decryption of an electronic device as a "*Gelfgatt* motion").

[39] *Gelfgatt*, 468 Mass. at 517.

[40] *Id.* at 517–18.

[41] *Id.* at 514.

[42] *Id.* at 522.

[43] *Id.*

Once the Court determined that the Fifth Amendment might protect the compelled testimony, it then analyzed whether the "foregone conclusion" doctrine stripped the act of decryption of its "testimonial character" (and thus its constitutional protection).[44] The Court stated that the doctrine requires the government to demonstrate its knowledge of (1) the existence of the evidence demanded; (2) the defendant's possession or control of such evidence; and (3) the authenticity of the evidence.[45] In *Gelfgatt*, the Commonwealth showed that the defendant claimed ownership and control of the computers during his interrogation, acknowledged that the computers were encrypted, and admitted he knew the encryption key.[46] Therefore, the factual statements conveyed to the Commonwealth from the defendant's decryption would be a "foregone conclusion" because they would merely reveal information the government already possessed.[47] Accordingly, the SJC agreed with the Commonwealth that the "foregone conclusion" exception applied, concluding that compelling a defendant to unlock an encrypted device did not violate the Fifth Amendment if the decryption did not relate testimonial facts to the government beyond what the defendant had already revealed to investigators.[48]

## II. *Commonwealth v. Jones*

### A. *Factual Background*

The defendant, Dennis Jones ("Jones"), was ultimately convicted by a grand jury for trafficking a person for sexual servitude,[49] in violation of Mass. Gen. Laws. ch. 265, § 50(a),[50] and deriving support from the earnings of a prostitute,[51] in violation of Mass. Gen. Laws. ch. 272, § 7.[52] The police arrested Jones shortly after his former girlfriend, Sara,[53] reported that Jones stole her purse and, upon the officers' arrival, revealed Jones was operating

---

[44] *Id.*

[45] *Gelfgatt*, 468 Mass. at 522.

[46] *Id.* at 523–24.

[47] *Id.* at 523.

[48] *Id.* at 514.

[49] Commonwealth v. Jones, 481 Mass. 540, 541 (2019).

[50] MASS. GEN. LAWS ANN. ch. 265, § 50(a) (West 2012) (making it a crime for someone to knowingly entice another person to engage in commercial sexual activity).

[51] *Jones*, 481 Mass. at 541.

[52] MASS. GEN. LAWS ANN. ch. 272, § 7 (West 2021) (making it a crime for someone who, knowing a person is a prostitute, lives, derives support, or shares, "in whole or in part, from the earnings or proceeds of his prostitution, from moneys loaned, advanced to or charged against him" by any manager or inmate of a place where prostitution is practiced or allowed).

[53] *Jones*, 481 Mass. at 543 n.4 (noting that Sara is a pseudonym).

a human trafficking ring.[54] Sara told the police that she met Jones through an online dating website a few weeks prior to the arrest.[55] Sara was initially under the impression that the two were dating, but Jones quickly persuaded her to work as a prostitute in exchange for housing.[56]

The police then began investigating Jones, linking him to an LG brand cell phone ("LG phone").[57] Sara informed the police that Jones primarily used the LG phone to communicate with her, and a subsequent inspection of Sara's cell phone confirmed several prostitution related messages between the two phones.[58] Sara explained that both Jones and a female associate regularly used the LG phone to conduct their prostitution business.[59] The police further discovered a website advertising Sara as an escort that listed the LG phone number as the principal point of contact for prospective customers.[60] The police recovered two phones from Jones upon his arrest, ultimately finding the LG phone in Jones's pants pocket.[61]

B. *Procedural History*

The police were granted a warrant to search the LG phone during the investigation, but the phone's contents were encrypted, making them inaccessible.[62] The Commonwealth then filed a *Gelfgatt* motion to compel Jones to unlock the LG phone by entering in its password, causing Jones to raise his Fifth Amendment right against self-incrimination.[63] The Commonwealth argued that compelling Jones to enter the password did not implicate the Fifth Amendment because "the act itself would not reveal any information that the Commonwealth did not already know."[64] A judge disagreed and denied the *Gelfgatt* motion, concluding that the Commonwealth did not demonstrate with "reasonable particularity" that Jones's knowledge of the password was a "foregone conclusion."[65] A renewed *Gelfgatt* motion with additional evidence was similarly denied

[54] *Id.* at 542.

[55] *Id.* at 543.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Jones*, 481 Mass. at 543–44 (explaining that Jones responded to text messages, while the female associate answered phone calls).

[60] *Id.* at 544.

[61] *Id.*

[62] *Id.*

[63] *Id.* at 545.

[64] *Id.*

[65] *Jones*, 481 Mass. at 545.

several months later.[66]

The Commonwealth thereupon filed for relief under Mass. Gen. Laws. ch. 211, § 3,[67] and the case was reported by the single justice to the SJC to address three specific issues.[68] First, the Court had to determine the necessary burden of proof that the Commonwealth bears on a *Gelfgatt* motion in order to establish a "foregone conclusion."[69] Second, it had to determine whether the Commonwealth met that burden in this case.[70] Third, the SJC had to determine whether a judge, before considering any additional information included in a renewed *Gelfgatt* motion, must initially find that the additional information was not known or reasonably available to the Commonwealth when the first motion was filed.[71]

C. *The SJC's Analysis*

Before addressing the three reported issues, the SJC created an analytic framework to establish when an individual can invoke the right against self-incrimination in response to a *Gelfgatt* motion.[72] The Fifth Amendment applies when the government compels an individual to produce evidence that constitutes an incriminating testimonial communication.[73] Following *Gelfgatt*, a court looks to "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" in order to determine whether an act of production is testimonial.[74] The SJC concluded that unlocking an electronic device says nothing about the contents of the device, nor does it produce any evidence for the Commonwealth beyond the fact that the defendant knows the password to the device.[75] Put simply, the SJC determined that compelling the defendant to enter the password into a computer could be a testimonial act of production, unless the facts conveyed by the defendant through this act of decryption were already known to the

---

[66] *Id.* at 556–57 (noting that the Commonwealth offered additional evidence that Jones possessed the phone at the time of his arrest: Jones listed the LG phone number as his own during a previous, unrelated arrest; the backup telephone number registered for the LG phone belongs to Jones; and the LG phone has been in the same location as another cell phone belonging to Jones).

[67] MASS. GEN. LAWS ANN. ch. 211, § 3 (West 2012).

[68] *Jones*, 481 Mass. at 542.

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.* at 547–49.

[73] *Id.* at 545.

[74] *Jones*, 481 Mass. at 546 (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 520 (2014)).

[75] *Id.* at 547.

Commonwealth, and thus were a "foregone conclusion."[76] Therefore, for the "foregone conclusion" exception to apply to a *Gelfgatt* motion, the Commonwealth need only demonstrate that the defendant knew the password to the LG phone.[77]

The SJC determined that the Commonwealth must prove a defendant knows the password beyond a reasonable doubt,[78] concluding that the Commonwealth satisfied its burden in this case.[79] The SJC further concluded that a judge acting on a renewed *Gelfgatt* motion may consider additional information without initially requiring the Commonwealth to show that the information was not known or reasonably available when the earlier motion was filed.[80] Accordingly, the SJC found that the motion judge abused his discretion by failing to consider the Commonwealth's renewed *Gelfgatt* motion and its additional information.[81] The SJC reversed the motion judge's denial of the renewed *Gelfgatt* motion and remanded the case to the Superior Court to enter a *Gelfgatt* motion compelling Jones to unlock the LG phone.[82]

D. *Concurring Opinion*

In a concurrence, Justice Lenk agreed with the outcome of the case but believed that entering the password to the phone revealed more than mere knowledge of the password.[83] Accordingly, the government should have been required to show, with reasonable particularity, that the defendant knew the password and that the government knew of the existence and location of incriminating evidence on the device.[84]

## ANALYSIS

### III. Mistaken Interpretation of Testimonial Communication

A. *The Password Is Not the Only Testimonial Communication*

An act of production is testimonial for purposes of the Fifth Amendment

---

[76] *See id.*

[77] *Id.* at 543.

[78] *Id.*

[79] *Id.* at 557–58 (reasoning that the additional evidence in the renewed *Gelfgatt* motion coupled with Sara's statements demonstrated Jones's knowledge of the password beyond a reasonable doubt).

[80] *Jones*, 481 Mass. at 558.

[81] *Id.* at 558–59.

[82] *Id.* at 561.

[83] *See id.* at 561 (Lenk, J., concurring).

[84] *Id.* at 565–66 (Lenk, J., concurring).

if "the government compels the individual to disclose the contents of his [or her] own mind to explicitly or implicitly communicate some statement of fact."[85] The SJC stated that the only testimony conveyed in the context of compelled decryption is that "the defendant knows the password . . . . The entry would convey no information about the contents of the LG phone."[86] Although the SJC is correct that entering the password discloses the fact that the defendant knows the password, this Comment will explain that the password is not the only testimony conveyed.[87] Moreover, the conclusion that the contents of the phone would not be conveyed by requiring decryption cannot coincide with the definition of testimonial communication provided by the SJC.[88]

1. If Unlocking the Phone Does Not Convey its Contents, Then Why Does the Commonwealth Want the Password?

The testimony conveyed by entering a password into a phone is not merely the password but also includes additional statements of fact that this decryption explicitly or implicitly communicates.[89] The SJC itself concluded that the "Commonwealth must be certain that the compelled act of production will not implicitly convey facts not otherwise known to the Commonwealth."[90] However, the SJC only used this principle to justify raising the burden of proof to beyond a reasonable doubt.[91] Had it applied this reasoning during its "foregone conclusion" analysis, the SJC would have realized that the compelled production of a password implicitly conveys evidence that the Commonwealth did not already know.[92]

By entering a password to a device, an individual also conveys control of the device, and therefore knowingly admits possession of the incriminating documents found on it.[93] Producing the password accords the implicit communication of these documents with protection under the Fifth Amendment because they are "reflective of the knowledge, understanding, and thoughts" of the defendant.[94] Moreover, the moment the defendant

---

[85] *Id.* at 546 (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 520 (2014)).

[86] *Jones*, 481 Mass. at 548 n.10; *see also* Kerr, *supra* note 6 at 769–70 (arguing that the only testimony conveyed is that the individual who unlocked the device knows the password).

[87] *See infra* Part III(A)(1)–(2).

[88] *See infra* Part III(A)(2).

[89] *See* Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 225, 229–30 (2018).

[90] *Jones*, 481 Mass. at 555.

[91] *See id.*

[92] *See id.*; Sacharoff, *supra* note 89, at 231.

[93] Sacharoff, *supra* note 89, at 229.

[94] *Jones*, 481 Mass. at 546.

unlocks the device, it is more likely that the material found on it belongs to the defendant and no one else.[95] Since the Commonwealth did not compel Jones to produce specific, relevant evidence on the LG phone,[96] it did not demonstrate that the testimony conveyed by Jones entering the password was a "foregone conclusion."[97]

By filing a *Gelfgatt* motion, the government essentially requires the defendant to "enter his password to the device and walk away," giving the government virtually unlimited access to the defendant's "entire digital life."[98] As it stands now, this unlimited access could allow the government to probe around for evidence of new crimes.[99] According to the SJC's conclusion, the government can force a defendant to enter the password in any case in which it can prove the defendant owns the device.[100] This conclusion permits the government to search a defendant's entire digital life for evidence of new crimes supposedly without violating the Fifth Amendment.[101] This goes against a fundamental principle of the Fifth Amendment that the government must "shoulder the entire load" in building its case against the defendant.[102] Therefore, the password should not be the only focus of analysis when applying the "foregone conclusion" doctrine.[103]

The *Gelfgatt* Court stated that entering a password to a device implicitly admits ownership and control of the device and its contents, as well as communicates "knowledge about particular facts that would be relevant to the Commonwealth's case."[104] In *Gelfgatt*, the Commonwealth listed the exact documents in its search warrant, negating any need to consider what would happen if the Commonwealth did not know which facts conveyed

---

**95** *See* Sacharoff, *supra* note 89, at 231 ("The moment the suspect opens [the smartphone], in this context, makes it more likely the child pornography is his and not someone else's.").

**96** *Jones*, 481 Mass. at 548 n.10.

**97** *See* United States v. Doe, 670 F.3d 1335, 1347 (11th Cir. 2012) (holding that the government must show it possessed knowledge as to the "files on the [encrypted] hard drives at the time it attempted to compel production"); Sacharoff, *supra* note 89, at 229.

**98** Sacharoff, *supra* note 89, at 208; *see* Commonwealth v. Gelfgatt, 468 Mass. 512, 517–18 (2014).

**99** *See* Sacharoff, *supra* note 89, at 208.

**100** *Jones*, 481 Mass. at 557.

**101** *See id.* at 557–58.

**102** United States v. Balsys, 524 U.S. 666, 690 (1998) (quoting Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964)).

**103** *See* United States v. Apple MacPro Comput., 851 F.3d 238, 247–48 (3d Cir. 2017); Eunjoo Seo v. State, 148 N.E.3d 952, 957–58 (Ind. 2020) (finding that, for the "foregone conclusion" to apply, the state must show that (1) the suspect knows the password to the phone; (2) the files on the device exist; and (3) the suspect possessed those files).

**104** Commonwealth v. Gelfgatt, 468 Mass. 512, 522 (2014).

would be relevant to its case.[105] This is distinguishable from *Jones* where the Commonwealth did not know what relevant evidence it would encounter once Jones entered the password.[106] The Commonwealth merely wanted to conduct a search of "the entire phone, all contacts, calendar entries, files, photographs, videos, caller-ids, text messages, voice mails, email messages and the contents of all of the above to *identify the 'regular user of the phone.'*"[107]

In defense of its *Gelfgatt* motion, the Commonwealth argued that password entry was necessary to execute the search warrant to identify the user of the LG phone.[108] The Commonwealth claimed that the *Gelfgatt* motion did not violate the Fifth Amendment because, as Jones was a regular user of the phone, it was a "foregone conclusion" that he knew the password.[109] To put it another way, the Commonwealth wanted to search the LG phone to determine who controlled it, but claimed that compelling Jones to unlock the LG phone would not violate the Fifth Amendment because the Commonwealth knew that he controlled it.[110] Actual application of the Commonwealth's illogical reasoning renders the search warrant completely unnecessary because the Commonwealth claimed it already knew Jones was the "regular user of the phone."[111] The success of this circular reasoning further supports the argument that greater protection is needed because it subjects the device to a "fishing expedition," which the Fifth Amendment aims to limit.[112]

2. An English Lesson

The SJC's conclusion that the password is the only testimony conveyed runs afoul with the Court's own definition of testimonial communication.[113] The SJC defined an act of production as testimonial if "the government compels the individual to disclose the contents of his [or her] own mind to explicitly or implicitly communicate some statement of fact."[114] When a sentence is structured as "to [blank] to [blank]," the reader cannot simply

---

[105] *Id.* at 520 (stating that the Commonwealth "believes that those devices contain information about the defendant's alleged mortgage payoff scheme").

[106] *See* Brief of the Appellee at 9, Commonwealth v. Jones, 481 Mass. 540 (2019) (No. SJC-12564) (showing that the Commonwealth's search warrant was to identify the user of the phone and not to locate certain incriminating evidence).

[107] *Id.* (emphasis added).

[108] *See id.*; Commonwealth v. Jones, 481 Mass. 540, 544 (2019).

[109] *See Jones*, 481 Mass. at 556–57.

[110] Brief of the Appellee, *supra* note 106, at 9.

[111] *See Jones*, 481 Mass. at 542, 556–57; *see also* Brief of the Appellee, *supra* note 106, at 9.

[112] *See* Sacharoff, *supra* note 89, at 208.

[113] *See Jones*, 481 Mass. at 546.

[114] *Id.* (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 520 (2014)).

chop it off halfway and ignore the second half of the sentence.[115] The second half of the sentence is the precise purpose of the proposition.[116] Take, for example, the following statement: "I gave ten dollars to Amy to bake cookies."[117] The speaker of this sentence gave Amy ten dollars *in order to* bake cookies.[118] Applying this same reasoning to testimonial communication, it is apparent that the defendant disclosed the evidence *in order to* communicate some statement of fact.[119]

In the context of compelled decryption, the evidence disclosed is the password itself because that is literally what the government compels.[120] This disclosure must further "explicitly or implicitly communicate some statement of fact."[121] The statement of fact cannot be the password itself, because that is what the defendant disclosed.[122] It stands to reason that the statements of facts implicitly communicated are the actual contents of the phone.[123]

Consider the following analogy: the act of entering a password to a decrypted phone in order to help the government execute a search warrant is comparable to the act of producing documents in compliance with a subpoena.[124] To force a defendant to produce subpoenaed documents, the Court does not ask the government to demonstrate that the defendant is physically capable of doing so.[125] Rather, the government is required to show that the documents exist and are in the defendant's possession.[126] Applying this same principle to compelled decryption, the government must show that the underlying documents on the device exist, not that the defendant

---

**115** *See To, In Order To, So As To*, ENG. GRAMMAR (Jan. 21, 2014), https://perma.cc/UK3M-Q9NT.

**116** *See Infinitives of Purposes*, GRAMMAR LAB, https://perma.cc/Z3LP-5PC7 (last visited Oct. 16, 2021) ("We use infinitives of purpose to say why someone does something.").

**117** *Cf. id.* ("They are going to the grocery store to buy some milk.").

**118** *See id.*

**119** *See id.* ("We use infinitives of purpose to say why someone does something.")

**120** *See, e.g.*, Commonwealth v. Jones, 481 Mass. 540, 547 n.9 (2019) (stating that the Commonwealth "requested that the defendant 'produce' or 'provide' the password to the LG phone").

**121** *Id.* at 546 (quoting Commonwealth v. Gelfgatt, 468 Mass. 512, 520 (2014)).

**122** *Id.* at 561 (compelling defendant to enter the password to the phone).

**123** *See* Sacharoff, *supra* note 89, at 232 (arguing that, in the context of encryption, "the government must show it can authenticate the files independently of the defendant's act of entering the password").

**124** Sacharoff, *supra* note 89, at 229.

**125** Sacharoff, *supra* note 89, at 237.

**126** Sacharoff, *supra* note 89, at 236.

knows the password and therefore is capable of entering it.[127] In the context of compelled decryption, the password itself is not produced; instead, the act of entering the password produces the documents on the electronic device.[128] These contents produced must be given Fifth Amendment protection.[129]

B. *Conclusion Alone Prohibits Assertion of the Fifth Amendment*

The Fifth Amendment only applies when the defendant "is compelled to make a testimonial communication that is incriminating."[130] The SJC concluded that the *only* testimony conveyed by compelling Jones to enter the password is that he knows the password.[131] This conclusion itself prohibits assertion of the Fifth Amendment because a password alone is not incriminating.[132] In other words, while the act of entering the password is sufficiently testimonial, the password itself is not incriminating.[133] If the SJC is correct that the password is the only testimony conveyed, then entering the password does not satisfy the requirements to invoke the Fifth Amendment.[134]

Despite concluding that the only evidence at issue is the password, the SJC created an analytic framework requiring the Commonwealth to prove that the defendant's knowledge of the password to the device is a "foregone

---

[127] *See* Sacharoff, *supra* note 89, at 236.

[128] Sacharoff, *supra* note 89, at 237.

[129] *See* Sacharoff, *supra* note 89, at 236–37 ("If the government cannot identify any documents on the device, the suspect's compelled act—entering the password—will communicate to the government the person's possession of the documents and their authenticity, facts the government did not know previously.").

[130] Fisher v. United States, 425 U.S. 391, 408 (1976).

[131] Commonwealth v. Jones, 481 Mass. 540, 547 (2019).

[132] *See* United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *54 (N.D.N.Y. May 24, 2006) (discussing the government's argument that the password itself is not incriminating); United States v. Mitchell, 76 M.J. 413, 421 (C.A.A.F. 2017) (Ryan, J., dissenting) (reasoning that even if unlocking an iPhone "could constitute a *testimonial* statement, the entry of a passcode . . . does not constitute an *incriminating* statement"); Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 197.

[133] Reitinger, *supra* note 132, at 197–98 (finding that a password is not compelled testimonial evidence because its contents are not privileged; rather, using the password to unlock the incriminating encrypted document makes the act of producing the password testimonial and incriminating); *see Mitchell*, 76 M.J. at 421 (Ryan, J., dissenting).

[134] *See* United States v. Castro, 129 F.3d 226, 229 (1st Cir. 1998) (noting that the defendant must "open himself to prosecution" by testifying in order to invoke the privilege against self-incrimination); In re Enforcement of a Subpoena, 435 Mass. 1, 3 (2001) (finding that the compelled evidence must subject the individual to criminal liability in order to assert the Fifth Amendment).

conclusion."[135] The SJC essentially concluded that the Fifth Amendment did not apply, and created an analytic framework requiring the Commonwealth to show then that the Fifth Amendment did not apply.[136] Applying a "foregone conclusion" analysis, an exception to the Fifth Amendment, to a non-incriminating testimonial communication illustrates that the SJC misinterpreted the definition of testimonial communication.[137] To logically defend the creation of this framework, the SJC must concede either that the password is incriminating or that the password conveys testimonial facts that are incriminating.[138] The former does not coincide with the accepted fact that a password alone is not incriminating,[139] whereas the latter derives considerable support from the growing body of literature regarding compelled decryption of electronic devices.[140] Since the password alone cannot trigger the Fifth Amendment, it stands to reason that the Commonwealth compelled incriminating testimony other than the password.[141]

### C. *The SJC Ignored the Purpose Behind the "Foregone Conclusion" Doctrine*

The Fifth Amendment only protects compelled testimonial communications that are incriminating.[142] The government can negate this constitutional protection by demonstrating that the facts conveyed by the compelled act are a "foregone conclusion."[143] The U.S. Supreme Court in *Fisher* stated that compelling the defendant to admit the existence and possession of certain tax papers was a "foregone conclusion" because the

---

[135] *Jones*, 481 Mass. at 547–48.

[136] *Id.*

[137] *See generally* Fern L. Kletter, Annotation, *Construction and Application of "Foregone Conclusion" Exception to Fifth Amendment Privilege Against Self-Incrimination*, 25 A.L.R. FED. 3D Art. 10 (Westlaw through Oct. 16, 2021).

[138] *See* Cuadra v. State, 715 S.W.2d 723, 725 (Tex. Crim. App. 1986) ("Only incriminating, *testimonial* communications are privileged.").

[139] *See* United States v. Suarez, Army Misc. 20170366, 2017 CCA LEXIS 631, at *8 n.3 (A. Ct. Crim. App. Sep. 27, 2017) (stating that the government maintains a passcode is not incriminating); Reitinger, *supra* note 132, at 188–89 (noting that a password will not be incriminating unless the government used "that fact to show possession or control over other encrypted documents not involved in the act of production, such as other encrypted documents the government had previously seized").

[140] *See, e.g.*, Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 TEX. L. REV. ONLINE 73, 74 (2019); Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 169, 174 (2018); Sacharoff, *supra* note 89, at 229.

[141] *See generally Cuadra*, 715 S.W.2d at 725.

[142] *Id.*

[143] Fisher v. United States, 425 U.S. 391, 411 (1976).

"taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[144] When applying the "foregone conclusion" doctrine to the compelled decryption of electronic devices, the SJC narrowly interpreted the *Fisher* Court's ruling to mean that "the facts conveyed" only applied to the password.[145] The SJC ultimately concluded that the Commonwealth proved beyond a reasonable doubt that Jones had knowledge of the password to the LG phone.[146] Therefore, the knowledge of the password was a "foregone conclusion," and Jones was not entitled to the protections of the Fifth Amendment.[147]

By ignoring the line that the facts conveyed must "add little or nothing to the sum total of the government's information," the SJC completely changed the meaning and ignored the purpose of the "foregone conclusion" doctrine.[148] The U.S. Supreme Court implemented the "foregone conclusion" doctrine to apply in scenarios where the compelled evidence does not contribute to the government's case.[149] However, the SJC's determination that the foregone conclusion only applies to the defendant's knowledge of the password created an avenue for the government to gain access to a significant amount of new and incriminating information that would, in fact, help build the government's case.[150]

## IV. Proposed Resolution

This issue deserves attention from the U.S. Supreme Court in that a federal standard is necessary to safeguard this fundamental right.[151] To invoke the "foregone conclusion" doctrine, the government must show with reasonable particularity it already knew of the subpoenaed materials at the time of the request.[152] Therefore, a *Gelfgatt* motion should require the Commonwealth to show with reasonable particularity that the existence and location of incriminating documents on a device are a "foregone

---

144 *Id.*

145 Commonwealth v. Jones, 481 Mass. 540, 546–47 (2019).

146 *Id.* at 557.

147 *Id.* at 558.

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

149 *See id.*

150 *See* Sacharoff, *supra* note 89, at 208.

151 *See generally* U.S. CONST. amend. IV.

152 United States v. Doe, 670 F.3d 1335, 1345–46 (11th Cir. 2012) ("[U]nder the 'foregone conclusion' doctrine, an act of production is not testimonial . . . 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.'").

conclusion."[153]

If the government is not required to show that a device contains particular facts relevant to its case, then we are essentially giving the government access to go blindly hunting in hopes of finding incriminating evidence to build its case.[154] On top of that, we are forcing the hunted individual to hold the government's hand and guide the way.[155] This goes against the very purpose of the Fifth Amendment: to protect individuals from being forced to provide testimony that is then used against them by the government.[156]

This Comment proposes that, if the government attempts to execute a search warrant to a device containing incriminating information by compelling a defendant to decrypt it and that defendant subsequently raises a Fifth Amendment right against self-incrimination, the government must initially demonstrate there are no other reasonable means available to unlock the device.[157] Additionally, the government must show with reasonable particularity: (1) the location and existence of incriminating evidence on the device; (2) the government's knowledge of the defendant's control and ownership of the device; and (3) the government's knowledge that the defendant knows the password.[158] The defendant should then decrypt only the incriminating evidence that the government proved to exist with reasonable particularity.[159]

To be clear, this proposed resolution does not require the government to state in its search warrant the files it wants to search with reasonable particularity.[160] However, if the defendant subsequently raises a Fifth Amendment right against self-incrimination, then the government must show with reasonable particularity its knowledge of the files to rebut this constitutional protection.[161] While it may be simpler to hold that the Fourth

---

[153] *Id.* at 1346.

[154] *Cf.* United States v. Fox, 721 F.2d 32, 38 (2d Cir. 1983) (reasoning that the government's "broad-sweeping summons" required the defendant to become the primary informant against himself, which is essentially a "fishing expedition").

[155] *See id.*

[156] *See* Miranda v. Arizona, 384 U.S. 436, 477–78 (1966) (stating that the purpose of the Fifth Amendment is to protect defendants from making incriminating statements as a result of governmental compulsion).

[157] *See* Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 208 (2014).

[158] *See Doe*, 670 F.3d at 1345–46; *see also* Commonwealth v. Gelfgatt, 468 Mass. 512, 521–22 (2014).

[159] Sacharoff, *supra* note 89, at 208.

[160] *See supra* text accompanying notes 157–59.

[161] *See supra* text accompanying notes 157–59.

Amendment will "somehow limit or trump the Fifth Amendment whenever there is a valid search warrant," these two rights should not be isolated from one another.[162] Rather, they must work together in order to consistently and adequately protect the rights of an individual.[163]

## CONCLUSION

Fundamental constitutional rights are diminished when the law fails to evolve with technology. An individual has a fundamental constitutional right against compulsory self-incrimination, but the SJC's holding in *Commonwealth v. Jones* effectively interred this right in the digital world. The decision to limit the applicability of the "foregone conclusion" doctrine to a defendant's knowledge of a password is a gross misinterpretation of the law. The U.S. Supreme Court introduced the "foregone conclusion" doctrine to compel incriminating testimony that adds little information to that which the government already possesses. However, the SJC with this decision gives the government virtually limitless access to individuals' electronic devices without requiring any prior demonstration of the government's knowledge of incriminating evidence on those devices.

The SJC inaccurately concluded that the act of unlocking a device does not implicitly convey its contents. This determination is both logically unsound and ignores the purpose of legal doctrine. In order for the government to succeed on a *Gelfgatt* motion, while simultaneously protecting the defendant's Fifth Amendment right, the government should be required to demonstrate with reasonable particularity the location and existence of incriminating evidence on the device and that the defendant controls the device and knows the password. Once the government demonstrates this, the defendant may then be compelled to decrypt only those files listed with reasonable particularity. Without federal implementation of these safeguards, an individual's right against self-incrimination in the digital world is essentially worthless.

---

[162] Commonwealth v. Jones, 481 Mass. 540, 564 n.1 (2019) (Lenk, J., concurring).

[163] *See id.*