COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

SJC-11358

COMMONWEALTH OF MASSACHUSETTS,
Plaintiff-Appellant,

v.

LEON GELFGATT,
Defendant-Appellee.

On Report of a Question of Law by the Superior Court for Suffolk County Pursuant to Mass. R. Crim. P. 34

BRIEF FOR *AMICI CURIAE* THE AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS, THE AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF THE DEFENDANT-APPELLEE

Matthew R. Segal (BBO#654489)
msegal@aclum.org
Jessie J. Rossman (BBO#670685)
jrossman@aclum.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS
211 Congress Street
Boston, MA 02110
Tel: (617) 482-3170
Fax: (617) 451-0009

Kit Walsh (BBO#673509)
cwalsh@cyber.law.harvard.edu
CYBERLAW CLINIC
BERKMAN CENTER FOR INTERNET AND SOCIETY
HARVARD LAW SCHOOL
23 Everett Street, 2nd Floor
Cambridge, MA 02138
Tel: (617) 495-7547
Fax: (617) 495-7641

Nathan F. Wessler (BBO#680281)
nwessler@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654

Hanni M. Fakhoury
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

INTRODUCTION

The Court has solicited briefs on the question whether the government may compel a criminal defendant to decrypt computers and other electronic storage devices. Under both the Fifth Amendment to the United States Constitution and article 12 of the Massachusetts Declaration of Rights, the government may not compel Massachusetts residents to testify or furnish evidence against themselves. Below, the Superior Court ruled that compelled decryption violates those commands because it requires a defendant to "assist the Government in understanding what seized materials mean." A363.

That ruling is correct. Encrypting electronic data does not simply lock it up; it scrambles the data into an unreadable format. Likewise, decrypting data does not simply unlock it; rather, decryption transforms scrambled data into readable data. Thus, as the Superior Court held, compelling someone to decrypt electronic data amounts to a command to explain the data. But, under the Fifth Amendment and article 12, that command is impermissible. The government cannot compel a defendant to turn unreadable data into data that can be used to put him in prison.

The Commonwealth misapprehends this reality. Most important, it asserts that requiring Gelfgatt to "decrypt his devices" would not require him to "produce decrypted files." Comm. Br. 26 n.9; Comm. Reply Br. 7-8 n.5. That is not so. Encrypting a device scrambles all of its files. By the same token, as the Commonwealth's own expert has acknowledged, decrypting that same device enables the automatic unscrambling of each and every file. See A64-68. Device decryption is quintessentially communicative because it yields unscrambled files that simply do not exist on the drive when it is encrypted.

Accordingly, this Court should hold that the compelled decryption of electronic devices implicates both the Fifth Amendment and article 12.

INTEREST OF THE *AMICI CURIAE*

The American Civil Liberties Union Foundation (ACLU) is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU Foundation of Massachusetts (ACLUM) is one of the ACLU's statewide affiliates. Both ACLUM and the ACLU, through its Project on Speech, Privacy, and

Technology, seek to protect the control that individuals have over their personal information. See, e.g., Commonwealth v. Augustine, No. SJC-11482.

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported digital civil liberties organization based in San Francisco, California, that works to protect privacy and free speech rights in an age of increasingly sophisticated technology. With more than 21,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and has served as an amicus in federal cases addressing how the Fifth Amendment applies to incriminating disclosure of encryption passwords and encrypted data, see In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); United States v. Decryption of a Seized Data Storage System, No. 2:13-mj-449-RTR (D. Wisc. 2013); and has served as amicus before this Court in cases applying constitutional protections to new technologies. See Commonwealth v. Augustine, No. SJC-11482; Commonwealth v. Rousseau, 465 Mass. 372 (2013).

BACKGROUND

The amici's understanding of encryption technology differs from the views advanced by the parties. The parties seem to dispute whether decrypting a computer drive is like disclosing the combination to a wall safe, as Gelfgatt seems to argue, or whether it is merely like entering the combination to the safe, as the Commonwealth contends. Compare Def. Br. 23-24, 29-30, with Comm. Br 36 n.12. In fact, decryption is not like either of those things.

Decryption is, instead, an act of translation and transformation. Being compelled to decrypt a computer drive is like being forced to create, for the benefit of someone standing on the steps of the Boston Public Library, an English translation of every single library book written in Braille. Doing so would not simply communicate the translator's access to and ability to translate the Braille works, though it would do that. It would also create new versions of those works: English translations revealing the number, length, and contents of all the books in the library's Braille collection.

Similarly, decrypting electronic data does not simply unlock information. It creates a new, intelligible version of that information.

I. Encryption

A. How Encryption Works

Encryption is, in essence, "the scrambling of information to disguise an intended communication." Black, Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy, 53 Fed. Comm. L.J. 289, 292 (2001). It allows for a plain text, readable message to be transformed into a seemingly incomprehensible format, readable only with the possession of an encryption "key" that can decrypt "the transformed message and return it to its original form." Id. Decryption is the process by which the transformed "ciphertext" is translated back into readable text. Gripman, Electronic Document Certification: A Primer on the Technology Behind Digital Signatures, 17 J. Marshall J. Computer & Info. L. 769, 774 (1999). Many people have used a system that encrypted their private information by entering a personal identification number into a bank ATM or by logging into a website with a username and password. Id. at 775.

Although computers use sophisticated algorithms to encrypt data, in principle that encryption resembles ciphers that can be encoded by hand. For example, using a "rotation" cypher to offset each letter in the alphabet by one, the phrase "Supreme Judicial Court" becomes "Tvqsfnf Kvejdjbm Dpvsu."

When information is encrypted on a computer, it exists only in its scrambled form. Unlike vaults and safes, which safeguard material by placing barriers around it, encryption safeguards data by transforming it into an unintelligible format. Thus, while the metaphor of a vault or safe might be useful in describing the security of encryption, it does not reflect the operation of the technology. See Gripman, supra, 17 J. Marshall J. Computer & Info. L. 769, at 774.

The Director of the Attorney General's Computer Forensic Laboratory, David Papargiris, has acknowledged how encryption really works. In an affidavit submitted to the Superior Court below, Papargiris did not claim that decrypting a file is like entering the combination to a safe. A64-68. To the contrary, he explained that encrypted data has been "scrambled in such a way as to render" it

unreadable. A64. Because encryption renders data into a new format, it is not identical to placing data inside a safe.

Just as encryption renders or transforms data, so too does decryption. Director Papargiris explained that "[d]ecryption is the process by which encrypted, scrambled data is rendered 'readable' again." Id. Although the information required to decrypt data is sometimes called a "key," see id., it does not function like a traditional key or the combination to a safe. Whereas a physical key unlocks some physical barrier to the sought-after material, an encryption program, in combination with the associated "key," transforms the sought-after material from encrypted nonsense into intelligible information. It is only by "funneling the encrypted data through the algorithm [that] the data is rendered 'readable' again." Id.

The "rotation" cypher above illustrates this point. Someone who knows both the algorithm--i.e., the rotation of letters--and the "key"--i.e., rotate one letter backward--can transform the phrase "Tvqsfnf Kvejdjbm Dpvsu" into "Supreme Judicial Court."

B. File Encryption versus Disk Encryption

Electronically-stored data can be encrypted in different ways. One option, known as "file encryption," encrypts only specified, individual files on a computer or other storage device. Another option, known as "drive encryption" or "disk encryption," encrypts all of the data occupying a specified storage area. E.g., TrueCrypt, System Encryption, at http://www.truecrypt.org/docs/system-encryption (last viewed Oct. 26, 2013).

For example, someone who opts for file encryption might choose to separately encrypt electronic copies of each tax return stored on her home computer, while leaving other files unencrypted. But someone who opts for disk encryption might encrypt the computer's entire hard drive. That approach would encrypt the tax return files as well as every other file on the drive, including the files for the computer's operating system.[1] Id.

---

[1] Another common form of encryption involves bundling some of a drive's files into an encrypted archive or encrypted volume. E.g., TrueCrypt, TrueCrypt Volume, at http://www.truecrypt.org/docs/truecrypt-volume (last viewed Oct. 26, 2013). Although this aggregate of encrypted files is itself stored as a single, encrypted file, for present purposes it is equivalent

Drive encryption deserves careful attention here because, according to the Commonwealth, it is the kind of encryption that has been applied to the devices seized from Gelfgatt. A66-67. Director Papargiris has asserted that these devices are "encrypted with Drive Crypt Plus full-disk, pre-boot encryption software." A67. If that is so, then the relevant devices, including every single file on them, are "encrypted 100%." Id. That is because disk encryption "automatically encrypts every bit of data that is entered or downloaded." Blackmer, Code or Clear? Encryption Requirements under Information Privacy and Security Laws, 26 No. 4 Corp. Couns. Q. art. 2 (2012).[2]

What is more, drive encryption makes it impossible to distinguish between encrypted data, on the one hand, and unused space, on the other. That is

---

to full disk encryption because it similarly obscures the properties of individual files as well as their content.

[2] See also Ries & Simek, Encryption Made Simple for Lawyers, 56-Apr. Res Gestae 24, 25 (2013) ("As its name suggests, full disk encryption protects the entire hard drive."); Symantec, White Paper: How Drive Encryption Works, at 1 (2012), http://www.symantec.com/content/en/us/enterprise/white_papers/b-how-drive-encryption-works_WP_21275920.pdf . ("Drive encryption protects a disk in the event of theft or accidental loss by encrypting the entire disk including swap files, system files, and hibernation files.").

because disk encryption programs typically fill free space with random data. For example, TrueCrypt's software "displays random characters if there are files and if there is empty space," thus obscuring "what, if anything, was hidden." In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1347 (11th Cir. 2012); see TrueCrypt, Hidden Volume, at http://www.truecrypt.org/docs/?s=hidden-volume (last viewed Oct. 21, 2013) ("free space on any TrueCrypt volume is always filled with random data when the volume is created and no part of the (dismounted) hidden volume can be distinguished from random data") (footnote omitted).

Just as drive encryption involves the wholesale scrambling of data, drive decryption involves the wholesale unscrambling of data. "Full disk encryption . . . automatically encrypts and decrypts all the data that travels in and out of the drive."[3] Although entering the key automatically makes

[3] Seagate, DriveTrust Technology: A Technical Overview, at 2, (2006), http://www.seagate.com/docs/pdf/whitepaper/TP564_DriveTrust_Oct06.pdf (emphasis added); see also Ries & Simek, Encryption Made Simple for Lawyers, supra n.1, at 25 ("The contents of the drive are automatically decrypted when an authorized user logs in").

decryption possible, it does not decrypt all of the files at once; instead, files are decrypted as access to them is sought, whether by the user or by a computer's operating system or software. This is true both in general and in the case of DriveCrypt Plus Pack (DCPP), the encryption software at issue here: "As data is read from the hard disk, DCPP automatically decrypts the data before it is loaded into memory. When data is written back to the hard disk, it is automatically re-encrypted."[4]

Thus, decrypting a drive furnishes information on the amount of data stored on the drive, the identities of the drive's files, and the contents of those files.

C. Encryption in Practice

Although the Commonwealth seeks to portray encryption as the exclusive province of criminals, legitimate encryption is common, responsible, and in

---

[4] SecurStar Computer Security, DriveCrypt Plus Pack Full Disk Encryption, http://www.securstar.com/products_drivecryptpp.php; see generally Symantec, How Drive Encryption Works, supra n.1, at 3. (emphasis added) ("When a user accesses a file, Drive Encryption decrypts the data in memory before it is presented for viewing. If the user makes any changes to the file, the data is encrypted in memory and written back to the relevant disk drive block just as it would be without encryption. Decrypted data is never available on the disk.").

some cases required by law. It is also vital for the protection of privacy in the modern world.

The personal computer has become a repository of private information, from personal journals to unpublished documents to pictures and videos to medical and financial records.[5] The private thoughts expressed in these types of papers have long been understood to be an extension of the person, as expressive of an individual's knowledge as may be retained within his head.[6] Storing those personal records securely with third parties risks exposing them to warrantless government surveillance based on the view, advanced by many governments, that information residing with third parties lacks constitutional protection. See Commonwealth v. Augustine, No. SJC-11482 (argued Oct. 10, 2013). Thus, encrypting data on personal electronic devices can be the only means of curbing government access. It can also protect against theft. A 2010 study of 329 private and public sector organizations reported that,

---

[5] See United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) ("Laptop computers, iPads and the like are simultaneously offices and personal diaries.").

[6] Fisher v. United States, 425 U.S. 391, 420 (1976) (Brennan, J. dissenting).

in one year, 86,455 laptops were lost or missing, averaging 263 laptops per organization.[7] Cyber attacks by both criminals and foreign governments have resulted in theft of large quantities of highly sensitive information.[8] If sensitive files are stolen through hacking or physical theft, encryption prevents the thief from ascertaining the files' contents.[9]

To protect the integrity and security of sensitive information, Massachusetts law requires encryption for laptops and portable storage devices that store or process personal data in connection with

---

[7] Erica Fruiterman, Upgrading the Fifth Amendment: New Standards for Protecting Encryption Passwords, 85 Temple L. Rev.655, 659 (2013), citing Ponemon Inst., The Billion Dollar Lost Laptop Problem: Benchmark Study of U.S. Organizations, 1 (Sept. 30, 2010), http://newsroom.intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf.

[8] See, e.g., Director Mueller on the Future of Cybersecurity, The FBI News Blog, http://www.fbi.gov/news/news_blog/director-mueller-on-the-future-of-cyber-security (last visited Oct. 22, 2013) ("[C]riminals are constantly discovering and exploiting vulnerabilities in our software and our networks.").

[9] See Shawn Henry, Exec. Ass't Dir., Federal Bureau of Investigation, Remarks, (Oct. 20, 2011), http://www.fbi.gov/news/speeches/responding-to-the-cyber-threat ("Managing the consequences of a cyber attack entails minimizing the harm that results when an adversary does break into a system. An example would be encrypting data so the hacker can't read it.").

business or employment;[10] and the U.S. Department of Commerce has also established best practices for the use of encryption.[11] Those commands have a rich history; many of the nation's founders, including Benjamin Franklin, James Madison, Thomas Jefferson, and Alexander Hamilton, "viewed cryptography as an essential instrument for protecting information, both political and personal."[12] In fact, Madison and Jefferson exchanged encrypted drafts of the Bill of Rights.[13]

Although encryption provides an added measure of privacy, that protection is not absolute. As acknowledged by Director Papargiris, law enforcement can decipher encrypted files by using cameras and keyloggers to capture a password, exploiting software bugs in the encryption technology, or guessing the password using "dictionary-based" and "heuristic" automated methods. A65. As a result, a motion to

---

[10] Mass. Gen. Law ch. 93H § 2; 201 CMR 17.00.

[11] See U.S. Dep't of Commerce, Computer Security Div., Nat'l Institute of Standards and Tech., Announcing the Advanced Encryption Standard (2001) (Federal Information Processing Standards Publication 197).

[12] Encryption As Constitutionally Protected Speech: Hearing Before the U.S. Judiciary Comm.'s Subcomm. on Constitution, Federalism and Property Rights, 105th Congress (1998) (statement of Cindy A. Cohn).

[13] Id.; see D. Kahn, The Codebreakers 185 (1967).

compel is not the only way in which the government can come to understand encrypted files. In Wisconsin, for example, the federal government has moved to dismiss an application to compel decryption because it successfully decrypted two hard drives without the defendant's assistance. See Mot. to Dismiss Application at 1, United States v. Decryption of a Seized Data Storage System, No. 2:13-mj-449-RTR (D. Wisc. filed Aug. 16, 2013), available at http://www.wired.com/images_blogs/threatlevel/2013/08/nodecryptfiling.pdf.

II. The Commonwealth's Motion to Compel

In this case, the Superior Court denied the Commonwealth's motion to compel defendant Gelfgatt to decrypt "each respective digital storage device" seized from his home by the Commonwealth. A47.

The Commonwealth had proposed that Gelfgatt accomplish this decryption by entering passwords or encryption keys into the devices, under circumstances that would preclude the Commonwealth from "view[ing] or record[ing] the password or key." A48. The Commonwealth also proposed that, generally speaking, it be "precluded from introducing [at trial] any

evidence relating to . . . the manner in which the digital media in this case was decrypted." Id.

But the Commonwealth's motion also sought to ensure that Gelfgatt would decrypt the drives in a manner of the Commonwealth's choosing. Recognizing that certain encryption keys can be set up to delete data, or to supply only some of the information that could be decrypted, the Commonwealth requested that Gelfgatt be ordered not "to destroy, change, or alter any data," or decrypt the drives in a manner that would "generate 'fake, prepared information.'" Id.

In support of its motion, the Commonwealth submitted Director Papargiris's affidavit, an audio recording of an interview with Gelfgatt, and three search warrants with accompanying affidavits. A49.

The Superior Court denied the Commonwealth's motion to compel but, at the Commonwealth's request, agreed to report the question now pending in this Court. A361, 366-67. The motion judge, Justice Raymond Brassard, reasoned that compelling Gelfgatt to decrypt the drives would violate the constitutional right against self-incrimination. First, Justice Brassard explained that the Commonwealth's order would require Gelfgatt to supply "meaningful access to materials

that the Government has obtained." A361-62. Second, Justice Brassard explained that compelled decryption is unlike the provision of physical evidence, which has been held not to violate the right against self-incrimination, and instead like the translation of a document, which does violate that right:

> I do not see how [compelled decryption] is any different than the following scenario: The Government obtains a search warrant for the personal effects of the defendant. The Government executes that warrant, and among other things, finds several pieces of paper, this could be 50 years ago, which appear to be in some sort of code, and/or several drawings that are entirely obtuse as to what their meaning is.
>
> Could the Government even though it had an interview with the defendant who acknowledged, yes, that's a code, yes those symbols have meaning, but I decline to provide them to you, could the Government force a defendant to provide such a code or such an explanation as to the meaning of drawings? I don't think so.
>
> I don't think the Constitution, federal or state, requires a defendant to in effect assist the Government in understanding what seized materials mean.

A362.

SUMMARY OF ARGUMENT

I. The privilege against self-incrimination, guaranteed by the Fifth Amendment and article 12, is implicated by government conduct involving (1) compulsion, (2) testimonial communication, and (3)

self-incrimination. The key issue here is whether compelled decryption of an electronic drive is testimonial. To answer that question, it is crucial to consider the key cases construing testimonial communications under the Fifth Amendment and article 12, and to consider the Eleventh Circuit's decision applying those cases in the context of decryption. Pp. 22-32.

I.A. Cases construing the Fifth Amendment and article 12 establish two key methods of determining when compelled conduct is not testimonial. First, conduct is not testimonial when it is a physical act that neither discloses nor demands the use of the contents of the defendant's mind. Thus, for example, giving a blood sample is not testimonial. Second, conduct arguably is not testimonial if the information it reveals is a "foregone conclusion" already known by the government. United States v. Hubbell, 530 U.S. 27, 44 (2000). Pp. 23-28.

I.B. Applying these methods of differentiating between testimonial and non-testimonial conduct, the Eleventh Circuit has held that the compelled decryption of electronic drives is testimonial. In re Subpoena Duces Tecum, 670 F.3d 1335. The court

observed that compelled decryption requires the use of the contents of a defendant's mind, and it reveals the defendant's possession of, access to, and control over the drives. Just as important, the Fifth Amendment protects both the information about the defendant's relationship with the encrypted drives and the content of the drives. Thus, the Eleventh Circuit held that, under the foregone conclusion doctrine, the government can compel decryption of a drive only when it seeks "a certain file" whose existence, location, and authenticity are already known by the government. Pp. 28-32.

II. The compelled decryption of an electronic drive is testimonial--and thus the files produced by such decryption are protected by the Fifth Amendment and article 12--for two separate and independent reasons. Pp. 33-44.

II.A. First, consistent with the Superior Court's ruling below, compelled drive decryption is testimonial because it requires the defendant to transform and explain the content of electronic data in the government's possession. Decryption transforms scrambled data into readable files, which literally changes the content on an encrypted device. For that

reason, even when a defendant does not turn over his decryption key to the government, the act of decryption is communicative in a way that unlocking a safe is not. Pp. 34-38.

The government's contrary argument hinges on the assertion that compelling a defendant to decrypt a drive does not compel the production of decrypted files. But that assertion is incorrect. Just as encrypting a drive encrypts each and every one of its files, decrypting the drive makes available decrypted copies of all of its files. Pp. 36-38.

II.B. Second, consistent with the Eleventh Circuit's ruling, compelled drive decryption is testimonial because it communicates facts about the defendant's relationship with the encrypted data. In particular, decryption communicates the existence of, access to and control over the drive's files. Thus, the Fifth Amendment protects the act of decryption. And because the Fifth Amendment requires derivative-use immunity, it also protects the content that is produced by the act of decryption. Pp. 38-41.

II.C. Relying on its mistaken view that drive decrypting does not produce decrypted files, the Commonwealth argues that it can invoke the foregone

conclusion doctrine without proving its knowledge of any particular files on Gelfgatt's drives. That is not so. Because drive decryption creates rather than unlocks content, and because derivative-use immunity protects the content of an encrypted device, any application of the foregone conclusion doctrine in this case will require the Commonwealth to establish knowledge concerning the content of the encrypted drives.

Three considerations bear on that issue. First, under this Court's article 12 cases, the foregone conclusion doctrine looks to whether a compelled communication would be trivial, and not just whether the information is known to the government. Second, under the Eleventh Circuit's test, the foregone conclusion doctrine requires the government to establish knowledge concerning "certain files." Third, this Court might wish to consider whether a "taint team" can or should protect the privileges that will be complicated by any decryption that might be ordered in this case. Pp. 41-44.

ARGUMENT

I. Compelled device decryption implicates the Fifth Amendment and article 12 because it is inherently testimonial.

The Fifth Amendment and article 12 protect Massachusetts residents from being compelled to provide testimonial communications, or to furnish evidence, against themselves. The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself." Fifth Amendment to the United States Constitution. It is implicated by government conduct that entails (1) compulsion, (2) a testimonial communication, and (3) self-incrimination. United States v. Hubbell, 530 U.S. 27, 34 (2000). Article 12 provides that "No subject shall . . . be compelled to accuse, or furnish evidence against himself." art. 12 of the Declaration of Rights of the Massachusetts Constitution. It "protects a person from being compelled to disclose the circumstances of his offence, the sources from which, or the means by which evidence of its commission, or of his connection with it, may be obtained, or made effectual for his conviction."

Emery's Case, 107 Mass. 172, 182 (1871); see Opinion of the Justices, 412 Mass. 1201, 1210 (1992). This Court has consistently held that article 12 provides a broader protection against self-incrimination than does the Fifth Amendment. See, e.g., id. at 1210; Commonwealth v. Doe, 405 Mass. 676, 678 (1989); Attorney Gen. v. Colleton, 387 Mass. 790, 796 (1982); Commonwealth v. Hughes, 380 Mass. 583, 595, cert. denied, 449 U.S. 900 (1980).

In this case, it is undisputed that the Commonwealth seeks to compel Gelfgatt to engage in conduct--namely, the decryption of several devices--that could incriminate him. So the relevant question is whether that conduct is testimonial. Federal and Massachusetts case law indicates that it is.

A. The Fifth Amendment and article 12 protect testimonial communications that are not foregone conclusions.

An act of production is testimonial if it requires someone "to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." In re Subpoena Duces Tecum, 670 F.3d at 1345, quoting Curcio v. United States, 354 U.S. 118, 128 (1957). For example, an act of production could reveal "that certain materials exist,

are in the subpoenaed individual's possession or control, or are authentic." Id. Similarly, this Court has explained that "'testimonial' evidence is evidence that 'reveals the subject's knowledge or thoughts concerning some fact.'" Commonwealth v. Lopes, 459 Mass. 165, 169-170 (2011), quoting Commonwealth v. Brennan, 386 Mass. 772, 777-778 (1982); see United States v. Wade, 388 U.S. 218, 223 (1967).

There are "two ways in which an act of production is not testimonial." In re Subpoena Duces Tecum, 670 F.3d at 1345. First, an act of production is not testimonial if it "merely compels some physical act, i.e. where the individual is not called upon to make use of the contents of his or her mind." Id. For example, producing the key to a lockbox containing documents is not testimonial. Hubbell, 530 U.S. at 43, citing Doe v. United States, 487 U.S. 201, 210 n.9 (1988). Nor is putting on a shirt, providing a blood sample, producing a handwriting exemplar, or making a voice recording.[14] Those actions do not relate to

[14] See United States v. Dionisio, 410 U.S. 1, 7 (1973) (voice exemplar); Gilbert v. California, 388 U.S. 263, 266 (1967) (handwriting exemplar); United States v. Wade, 388 U.S. 218, 222-223 (1967) (standing in a lineup); Schmerber v. California, 384 U.S. 757, 765

assertions of fact or belief or even a conscious process of recall. Hubbell, 530 U.S. at 35.

Second, an act of production is not testimonial--or at least not sufficiently testimonial--if it fits within what courts call the "foregone conclusion" doctrine. In re Subpoena Duces Tecum, 670 F.3d at 1345. As construed by several federal appeals courts, the "foregone conclusion" doctrine provides that a compelled act of production does not violate protections against self-incrimination if, at the time of production, the government already knows with "reasonable particularity" the contents of the materials being produced. Id. at 1344.[15] Under that standard, if "the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available."

(1966) (blood sample); Holt v. United States, 218 U.S. 245, 252-253 (1910) (wearing particular clothing).

[15] See United States v. Ponds, 454 F.3d 313, 320-321 (D.C. Cir. 2006); In re Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004); In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993).

Id.; see United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999) aff'd, 530 U.S. 27 (2000).

These principles do not supply "categorical answers." Fisher, 425 U.S. at 410. Instead, whether a compelled act of production is testimonial will depend on the specific facts of each case, and it often turns on what the government knew before compelling the production.

For example, in Fisher the government sought to compel the production of several taxpayers' documents that had been prepared by their accountants. 425 U.S. at 394-95. The documents were typical of those prepared in connection with tax returns, and the government already knew about their existence and location. Id. at 394, 411. Based on those facts, the Court held that their production was not testimonial because "the existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." Id. at 411. The Court made clear, however, that different circumstances could lead to the opposite conclusion. Id. at 410-11.

This prediction came to fruition in United States v. Hubbell, 530 U.S. 27 (2000). The defendant in that case had produced 13,120 pages of documents under an order, pursuant to 18 U.S.C. § 6003(a), that provided use and derivative-use immunity. Id. He challenged his ensuing indictment, claiming that the government violated the terms of the statute because all of its evidence was derived from the testimonial aspects of his production. Id. Because the scope of statutory immunity under § 6003 is co-extensive with the scope of the constitutional privilege against self-incrimination, id. at 38, the Court analyzed whether the production was testimonial under the Fifth Amendment.

The Court concluded that the production was indeed testimonial. Rejecting "the Government's anemic view of respondent's act of production as a mere physical act," the Court emphasized that Mr. Hubbell needed to "make extensive use of the contents of his own mind" to identify and assemble the hundreds of pages of documents. Id. at 43 (internal quotation marks omitted). Distinguishing Fisher, the Court also explained that the testimonial aspects of the production were not foregone conclusions:

> While in Fisher, the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent.

Id. at 45.

The Court warned that the Government could not cure this deficiency with the general argument that businessmen like Mr. Hubbell always possess the kinds of documents falling within the broad categories of the subpoena. Id.

B. The only pertinent appellate decision holds that compelled decryption of devices or drives is testimonial and not necessarily a foregone conclusion.

The only appellate court to apply these principles to decryption--the Eleventh Circuit--has unequivocally held that "decryption and production of the contents of . . . hard drives would sufficiently implicate the Fifth Amendment privilege." In re Subpoena Duces Tecum, 670 F.3d at 1346. In that case, an unnamed federal criminal defendant was served with a subpoena to produce the decrypted contents of certain hard drives and was granted immunity for the act of production but not for the derivative use of

the contents of the drives. Id. at 1349. He refused to comply with the subpoena and was held in civil contempt. The Eleventh Circuit reversed the contempt judgment based on three conclusions: (1) the subpoena compelled testimony because "Doe would certainly use the contents of his mind to incriminate himself or lead the Government to evidence that would incriminate him if he complied with [it]"; (2) the government could not invoke the "foregone conclusion" doctrine because it did not know with "reasonable particularity" that the sought-after files were on the drives; and (3) although the government had immunized Doe for the "act of production," the Fifth Amendment required that it also immunize Doe for "the contents of the production." Id. at 1349 & n.28, 1351-52.

As a threshold matter, the Eleventh Circuit reasoned that the "decryption and production" sought by the government would be testimonial. 670 F.3d at 1346. In particular, those acts "would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." Id. The court rejected the

government's view that no testimonial act would be compelled because the government did not "seek the combination or the key" itself. Id. That argument, the court noted, overlooked that in both Fisher and Hubbell the government also "sought the files being withheld, just as the Government does here." Id. Because "the decryption and production" sought by the government "demand[ed] the use of the contents of the mind," that conduct was "testimonial in character." Id.

In rejecting the government's reliance on the "foregone conclusion" doctrine, the court noted that "[n]othing in the record" showed that the government knew "whether any files exist[ed] and [were] located on the hard drive," or that the government knew "with reasonable particularity that Doe [was] even capable of accessing the encrypted portions of the drives. Id. The court also noted that, because "the TrueCrypt program displays random characters if there are files and if there is empty space," the Government "[did]

not know what, if anything, [was] held on the encrypted drives." Id. at 1347.[16]

For the foregone conclusion doctrine to apply, the court explained, the government would have to establish that it had "the requisite knowledge of what is contained" in the encrypted drives. Id. at 1347 n.25. The court held that the government did not necessarily "have to show that it kn[ew] specific file names." Id. at 1349 n.28. But, if it did not know a particular file name, the government would have to show "with some reasonable particularity that it seeks a certain file and is aware, based on other

[16] The Eleventh Circuit distinguished two district court cases where, in light of the government's extensive pre-production knowledge about the documents it sought, courts had applied the foregone conclusion doctrine. In re Subpoena Duces Tecum, 670 F.3d at 1348-49 & n.27; see United States v. Fricosu, 841 F. Supp. 2d 1232, (D. Colo. 2012) (holding existence and location of files were a foregone conclusion because the government introduced a recorded phone call where defendant admitted "it was on my laptop"); In re Grand Jury Subpoena to Sebastien Boucher, 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (unpub op) (holding existence and location of files were a foregone conclusion because the government had previously viewed the contents of some of the encrypted files). In In re Subpoena Duces Tecum, however, the Eleventh Circuit found no evidence "that the Government, at the time it sought to compel production, knew to any degree of particularity what, if anything, was hidden behind the encrypted wall." 670 F.3d at 1349.

information, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." Id.

Finally, the Eleventh Circuit held that the Fifth Amendment required that Doe be immunized not only for the act of production but also for the contents of the drive. Id. at 1351-52. It reasoned that the Supreme Court had already rejected the "manna from heaven" theory "which contended that if the government omitted any description of how the documents were obtained, it would be as if they magically appeared on the courthouse steps and the Government could use the documents themselves." Id. at 1352. Instead, the Supreme Court had held that the Fifth Amendment mandates both use and derivative-use immunity. Id. at 1351. The Eleventh Circuit explained that even if the contents of Doe's production were non-testimonial, allowing the government to introduce these documents would violate the Fifth Amendment "because doing so would allow the use of evidence derived from the original testimonial statement." Id. at 135152 (emphasis in original).

II. Compelled decryption is testimonial because it creates data and communicates information about the existence, possession, and control of that data, none of which is a foregone conclusion.

The Superior Court below and the Eleventh Circuit advanced two different reasons for concluding that compelled decryption is testimonial, and both are correct. First, because decryption creates new files--it does not simply hand over pre-existing files--the Superior Court correctly held that the compelled decryption of a drive actually compels an "explanation" of the drive's contents. A361-64. Second, because decryption communicates facts about a person's relationship with encrypted data--such as "his possession, control, and access" to encrypted portions of drives--the Eleventh Circuit correctly held that compelled decryption is "tantamount to testimony." In re Subpoena Duces Tecum, 670 F.3d at 1346. That court also concluded that, based on the government's lack of prior knowledge regarding the existence of any files, the encrypted portions of the drives were not foregone conclusions. Id. at 1346-49. In this case, this Court should endorse both of these approaches.

A. Compelled decryption is testimonial because it creates content.

The Superior Court was right: compelled decryption is testimonial because it requires a defendant to "assist the Government in understanding what seized materials mean." See A361-64. This rationale, which focuses on how decryption alters the content of electronic data, establishes that decryption is testimonial under both the cases interpreting the Fifth Amendment and under the more protective jurisprudence governing article 12.

1. Decryption transforms scrambled data into unscrambled data.

Decryption does not merely provide access to pre-existing data. Rather, it transforms pre-existing, scrambled data into data that can be understood. That act of transformation is fundamentally communicative. It communicates the number, size, and content of each and every file within the encrypted space. Moreover, because encryption tends to obscure the difference between content and empty space, decryption also communicates how much of a device is devoted to content and how much is empty space. Cf. In re Subpoena Duces Tecum, 670 F.3d at 1340, 1347.

The Commonwealth's submissions bear out that distinction between access and transformation. Although the Commonwealth argues that it seeks only to "access" pre-existing data on seized devices, see Comm. Op. Br. 20, its access to pre-existing data is already unfettered. Director Papargiris candidly acknowledged that the Commonwealth has a "bit by bit image of the seized media." A66. The Commonwealth's problem is that the existing bits are "unreadable." Id. So what the Commonwealth truly wants is to compel Gelfgatt to transform those bits into readable files that are not now present on any of the devices.

The Commonwealth's attempt to compel Gelfgatt to create files, though perhaps understandable, also confirms why decryption is not akin to the physical production cases on which the Commonwealth relies. In those cases, defendants were forced to deliver pre-existing physical evidence to the government. At best, those decisions would permit the Commonwealth to compel a criminal defendant to turn over the tattered remains of a confession that he handwrote and then ran through a document shredder. But those decisions would not permit the government to compel the defendant to reassemble the shredded document, even assuming he

could do so. That is because the reassembly would require the defendant to "use the contents of [the] mind" to provide incriminatory information. In re Subpoena Duces Tecum, 670 F.3d at 1345; see Hubbell, 530 U.S. at 43.[17]

In short, even assuming the Commonwealth could compel a criminal defendant to turn over a potentially-incriminating jigsaw puzzle--a generous assumption--it still could not compel the defendant to reassemble the puzzle. Yet that is essentially what the Commonwealth seeks to do in this case.

2. The Commonwealth overlooks that decrypting a device also decrypts and produces decrypted files.

The Commonwealth's contrary argument--that compelled decryption is not testimonial--expressly relies on a claim that compelling Gelfgatt to decrypt the seized devices would not require him to produce

---

[17] The Commonwealth also compares encryption to shredding, but it misapprehends the posture of this case by arguing that "one who is ordered to produce certain paper files is not allowed to first run them through a shredder." Comm. Br. 37. The relevant question is not whether a defendant individual can be prevented from shredding or encrypting a document after learning of an obligation to present the document to the government. Instead, the question is whether a defendant can be compelled to reassemble a document that was shredded or encrypted in the past, before any such obligation arose.

decrypted files. Comm. Op. Br. 26 n.9; Comm. Reply Br. 7-8 n.5. That claim is incorrect.

Compelling the decryption of a drive actually compels the production of decrypted files. Just as device encryption automatically encrypts all data on the device, device decryption "automatically decrypts" all data accessed by the user. See SecurStar Computer Security, DriveCrypt Plus Pack Full Disk Encryption, supra n.3. Thus, entering the "key" for an encrypted drive makes available unencrypted copies of each and every file on it. See generally supra nn.2-3. Even the Commonwealth's expert concedes that this is true; Director Papargiris has explained that, decrypting a computer "allow[s] the computer to decrypt." A66.

For that reason, device decryption will likely yield decrypted files having nothing to do with the underlying criminal investigation. Because device encryption can sweep up every file on the device--including files for the operating system--it is unlikely that each and every encrypted file will be relevant to a government subpoena or search warrant. Yet decrypting the device will enable decryption of all of those files, no matter whether they are

documents reflecting mortgage fraud or vacation photos of the defendant's family.

Decryption does not merely "unlock" those files. Nor does it merely "unlock" the device on which they reside. Instead, decryption creates unscrambled files from scrambled data. The Commonwealth's claim that device decryption can "provid[e] access" without "remaking" any files is simply incorrect. See Comm. Op. Br. 20. In fact, the opposite is true; the only way to access encrypted data is to remake it.

B. Compelled decryption is testimonial because it communicates information about a person's relationship to encrypted data.

For a separate and independent reason, the Eleventh Circuit was also right: compelled production is testimonial because it communicates facts about the relationship between the defendant and the devices and files being decrypted. Whereas the Superior Court's rationale points to the unscrambled content created and produced by decryption, the Eleventh Circuit's rationale points to non-content information that is conveyed by the act of decryption. But, significantly, the Eleventh Circuit's rationale equally indicates that the content itself is protected by the privilege against self-incrimination.

For starters, the Eleventh Circuit correctly observed that the decryption of a device and the consequential production of decrypted files "would be tantamount to testimony" that the defendant knows "the existence and location of potentially incriminating files"; that the defendant has "possession, control, and access to" encrypted data, and that the defendant has the "capacity to decrypt them." In re Subpoena Duces Tecum, 670 F.3d at 1346.

In response to those observations, the Commonwealth now advances the same argument that the government advanced in the Eleventh Circuit. Specifically, it "argue[s] that it does not seek the combination or the key," but rather the information that would be revealed by the act of decryption. Id.; see, e.g., Comm. Op. Br. 18-21. But the Eleventh Circuit concluded that this argument "badly misses the mark." In re Subpoena Duces Tecum, 670 F.3d at 1346.

That conclusion is accurate. As the Eleventh Circuit observed, the government never seeks a key "for its own sake." Id. Rather, in both Fisher and Hubbell, "the Government sought the files being withheld, just as the Government does here." Id. If the government could acquire such files simply by

disclaiming an interest in the information conveyed by the act of production, then the government could easily circumnavigate the privilege against self-incrimination in numerous cases. But that is not how the privilege operates. Instead, it turns on whether the act of production "demand[s] the use of the contents of the mind." Id. In the case of decryption, it does.

Relatedly, the Commonwealth's attempt to disclaim interest in Gelfgatt's actual decryption key overlooks that the privilege against self-incrimination demands both use and derivative-use immunity. Id. at 1349-52. In particular, "the Government cannot obtain immunity only for the act of production and then seek to introduce the contents of the production, regardless of whether those contents are characterized as nontestimonial evidence, because doing so would allow the use of evidence derived from the original testimonial statement." Id. at 1351-52.

In sum, the compelled decryption of electronic devices is testimonial both because it "re-makes" scrambled files and because it communicates facts about the defendant's relationship to the scrambled files. For either of those reasons, and certainly for

both of them, the Fifth Amendment and article 12 are implicated by such compelled decryption.

C. Compelled decryption is testimonial when the Commonwealth fails to establish that the content of the encrypted files is a foregone conclusion.

The Commonwealth argues that Gelfgatt's statements to investigators render his possession of, and ability to decrypt, the devices a foregone conclusion. Comm. Br. 26-27. Even if that is true, it does not address the question of whether the Commonwealth has any prior knowledge of the existence or location of any potential files on the devices. See In re Subpoena Duces Tecum, 670 F.3d at 1346. The Commonwealth argues that it need not answer this question--i.e., it does "not need to show any knowledge regarding any files"--in light of its assertion that compelling Gelfgatt to decrypt devices would not compel him to produce decrypted files. Comm. Br. 26 n.9; Comm. Reply Br. 7-8 n.5. But, again, that assertion is mistaken. Accordingly, the Commonwealth's present attempt to invoke the foregone conclusion doctrine cannot succeed. The amici respectfully submit that, if the Commonwealth now attempts to make some

showing regarding its knowledge of particular files, three considerations would be relevant.

First, it is unclear that any showing of knowledge with respect to particular files could permit the Commonwealth to invoke the "foregone conclusion" doctrine articulated in this Court's article 12 cases. Rather than focus on the "reasonable particularity" standard followed by several federal courts interpreting the Fifth Amendment, this Court has looked to whether the information that the Commonwealth seeks to compel "is 'trivial' and does 'not incriminate.'" Commonwealth v. Nadworny, 396 Mass. 342, 364 (1985); see also Commonwealth v. Hughes, 380 Mass. 583, 590, 592 (1980) (noting that the "information added" by the act of production in Fisher "was trivial"). Here, the decrypted files that would be made available by Gelfgatt's act of production would not be trivial; they are the substance of what the Commonwealth seeks.

Second, if this Court were to apply the "reasonable particularity" standard that federal courts have used when interpreting the Fifth Amendment, the Commonwealth would have to demonstrate that "it seeks a certain file and is aware, based on

other information, that (1) the file exists in some specified location, (2) the file is possessed by [Gelfgatt], and (3) the file is authentic." In re Subpoena Duces Tecum, 670 F.3d at 1349 n.28. In order to meet this standard, the Commonwealth must provide something more than the broad assertion that it expects certain general categories of documents to be on the device. See Hubbell, 530 U.S. at 45. Merely stating that the device could contain many files, or listing "categorical requests for documents the Government anticipates are likely to exist simply will not suffice." Id. at 1347. "[A]lthough the Government need not know the name of a particular file or account, it still must be able to establish that a file or account, whatever its label, does in fact exist." Id. at 1349 n.28.

Third, if this Court nevertheless concludes that some compelled decryption would be consistent with article 12 and the Fifth Amendment, it might wish to consider whether "taint team" procedures will be necessary or sufficient to protect Gelfgatt's rights. This Court has recently suggested that a taint team might be warranted when the Commonwealth's collection of information could intrude on a legal privilege. See

Preventive Medicine Assocs., Inc. v. Commonwealth, 465 Mass. 810 (2013). Here, the Commonwealth's review of decrypted files appears likely to intrude on the privilege against self-incrimination, because the devices at issue likely contain files that the Commonwealth cannot identify with reasonable particularity, and perhaps the attorney-client privilege, because Gelfgatt is an attorney.

CONCLUSION

Compelling a criminal defendant to decrypt electronic devices requires the defendant to use the contents of his mind--namely, his knowledge of a decryption key--to reassemble and unscramble information that can be used to incriminate him. For that reason, this Court should hold that such compelled decryption implicates the privileges against self-incrimination guaranteed by article 12 and the Fifth Amendment.

Respectfully submitted,

American Civil Liberties Union
Foundation of Massachusetts

American Civil Liberties Union Foundation

BY THEIR COUNSEL[18]

Matthew R. Segal (BBO#654489)
msegal@aclum.org
Jessie J. Rossman (BBO#670685)
jrossman@aclum.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
MASSACHUSETTS
211 Congress Street
Boston, MA 02110
Tel: (617) 482-3170
Fax: (617) 451-0009

Kit Walsh (BBO#673509)
cwalsh@cyber.law.harvard.edu
CYBERLAW CLINIC
BERKMAN CENTER FOR
INTERNET AND SOCIETY
HARVARD LAW SCHOOL
23 Everett Street, 2nd Floor
Cambridge, MA 02138
Tel: (617) 495-7547
Fax: (617) 495-7641

Nathan F. Wessler (BBO#680281)
nwessler@aclu.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654

Hanni M. Fakhoury
(CA# 252629)
hanni@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993

Dated: October 28, 2013

[18] Amici thank Harvard Law School Cyberlaw Clinic students Jane Li, Takayuki Matsuo, Shane O'Neal, Jillian Stonecipher, and Stella Unruh for their valuable contributions to this brief.

CERTIFICATE OF COMPLIANCE

I, Kit Walsh, hereby certify pursuant to Mass. R. App. P. 16(k) that the instant brief complies with the rules of court pertaining to the filing of briefs, including, but not limited to, Mass. R. App. P. 16(a)(6), (b), (e), (f), and (h), 18, and 20.

Dated: October 28, 2013 Kit Walsh

ADDENDUM

Constitution of the United States
Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Constitution of the Commonwealth of Massachusetts
Article XII

No subject shall be held to answer for any crimes or offence, until the same is fully and plainly, substantially and formally, described to him; or be compelled to accuse, or furnish evidence against himself. And every subject shall have a right to produce all proofs, that may be favorable to him; to meet the witnesses against him face to face, and to be fully heard in his defense by himself, or his council at his election. And no subject shall be arrested, imprisoned, despoiled, or deprived of his property, immunities, or privileges, put out of the protection of the law, exiled, or deprived of his life, liberty, or estate, but by the judgment of his peers, or the law of the land.

CERTIFICATE OF SERVICE

I, Kit Walsh, hereby certify that on September 23, 2013, I caused two true and correct copies of the above document to be served on counsel of record for each other party by mailing the document by first-class mail, postage pre-paid, to the following:

Counsel for Leon Gelfgatt:
Paul J. Davenport
Jeruchim & Davenport, LLP
Stanly D. Helinski
Helinski Law Offices
One McKinley Square, Fifth Floor
Boston, MA 02109

Counsel for the Commonwealth:
Randall E. Ravitz
Thomas D. Ralph
Assistant Attorneys General
Criminal Bureau
One Ashburton Place
Boston, MA 02108

Dated: October 28, 2013 Kit Walsh