5-2015

Forced Decryption as a Foregone Conclusion

Dan Terzian

California Law Review Circuit

Vol. 6 May 2015

Forced Decryption as a Foregone Conclusion

Dan Terzian*

INTRODUCTION

The argument runs like this. The Fifth Amendment generally bars forced incrimination. But under the foregone conclusion exception, the government can compel a person to produce anything (say, a car) where it reasonably knows the car exists. So too with encrypted computers.[1] The government can force a person to decrypt a hard drive because it always knows that an encrypted hard drive has a corresponding unencrypted version. Ergo, forcing decryption and production of a now-unencrypted computer is a foregone conclusion and, therefore, constitutional.

Courts have not explicitly engaged this argument. Yet they have implicitly engaged it—some accepting it, others rejecting—and not one has noted the growing split in decisions. Those accepting it follow my argument above; they require knowledge that the encrypted hard drive has an unencrypted version and then find the government knows this.

But for other courts, knowing that the unencrypted version exists isn't enough. Instead the government must also know particular files exist on that version. This method silently shifts the inquiry; facing the government's demand for a car (the unencrypted hard drive), these courts required knowledge of what's in the glove compartment (particular files). The shift is subtle, but the effect profound. Courts requiring only knowledge that the unencrypted version

* Associate, Duane Morris LLP.

[1] Or any other encrypted device.

exists will always find a foregone conclusion, whereas courts requiring knowledge of the particular files usually won't.

This shifted inquiry is wrong six times over. The courts adopting it did not explain why focusing on the subpoenaed item's contents prevails over the standard method of focusing on the subpoenaed item itself. Nor does examining five potential reasons compel or justify the shift.

I.
THE STANDARD METHOD AND THE FOREGONE CONCLUSION ARGUMENT

The privilege against self-incrimination, where applicable, grants a person the right to refuse "to be a witness against himself."[2] For the privilege to apply, the government must first seek to compel a "testimonial" response.[3] To be testimonial, a response requires one of two things: it must convey an implied communication (producing something implies you possessed it), or it must involve substantial mental effort.[4] What's substantial? Forcing someone to mine countless boxes for 13,000 pages of responsive documents is substantial,[5] while forcing mostly physical acts like providing a voice or handwriting sample is not.[6]

But finding a response testimonial does not automatically mean the privilege applies. Even if a response is testimonial, the privilege does not apply where the testimonial portion is a foregone conclusion.[7] This occurs where the

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

[3] *E.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012).

[4] *E.g.*, Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298, 304 (2014); Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 NW. U. L. REV. 56, 57–59 (2014).

[5] *See In re Grand Jury Subpoena*, 670 F.3d at 1345; *see also* United States v. Hubbell, 530 U.S. 27, 34–36, 41–42 (2000).

[6] *See* Fisher v. United States, 425 U.S. 391, 411 (1976) ("When an accused is required to submit a handwriting exemplar . . . his Fifth Amendment privilege is not violated because nothing he has said or done is . . . sufficiently testimonial."); *see also Hubbell*, 530 U.S. at 35.

[7] *In re Grand Jury Subpoena*, 670 F.3d at 1346 (holding that forced decryption was not a foregone conclusion because "nothing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives"); United States v. Ponds, 454 F.3d 313, 319–20 (D.C. Cir. 2006) (holding that the "'reasonable particularity' standard" applies even though the Supreme Court did not explicitly adopt it); *In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004) (holding that there was no foregone conclusion, even though the government "possessed extensive knowledge about Doe's price-fixing activities as a result of interviews," because the government did not have sufficient "knowledge of the existence and possession of the actual [subpoenaed] documents"); *see also Fisher*, 425 U.S. at 411; United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000) ("[T]he government must establish its knowledge of the existence, possession, and authenticity of subpoenaed documents with 'reasonable particularity' . . . .").

government knows "with 'reasonable particularity'" that the subpoenaed documents exist, that they're in a certain location,[8] and that they're authentic.[9]

Look closely, and note how these three requirements all target the same thing: "knowledge of . . . the actual documents, not the information contained therein . . . ."[10] So with a subpoena for "calendars, diaries, daybooks, [or] appointment calendars," the government must know of those documents.[11] Knowing only of "records establishing meetings"—presumably information contained within a calendar or daybook—isn't enough to get the calendars.[12]

Just as knowledge of the document's contents is irrelevant, so is knowledge of information related to the documents. Consider, for example, a subpoena for documents "regarding the 'use, ownership, possession, custody and/or control of a white Mercedes Benz.'"[13] The government must know those documents themselves exist, not just know that the person probably owned the Mercedes.[14]

The same should go for forced decryption. Subpoenas for the unencrypted version of an encrypted hard drive require knowing that the unencrypted version exists. Knowing particular files on the hard drive—whether the files are viewed as the drive's contents or as related information—is irrelevant because the files are not what was actually subpoenaed.

[8] Some courts have substituted the location requirement with the requirement that the respondent possess or control the documents, and some scholars have argued that this is the better approach. *See* United States v. Bright, 596 F.3d 683, 692 (9th Cir. 2010); *Ponds*, 454 F.3d at 324–25; Butcher v. Bailey, 753 F.2d 465, 469 (6th Cir. 1985) (stating that producing documents is testimonial where it "acknowledg[es] that they are in the control of the person producing them"); Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11, 23 (2012). If this approach prevails, my analysis does not change. The government will prove possession just as it proves authentication, by showing that the computer was in the respondent's home. *See infra* notes 16–19 and accompanying main text.

[9] *See In re Grand Jury Subpoena*, 670 F.3d at 1344 ("Where 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." (footnote omitted)); *In re Grand Jury Subpoena*, 383 F.3d at 910 ("[T]he government was required . . . to establish the existence of the documents sought and Doe's possession of them with 'reasonable particularity' before the existence and possession of the documents could be considered a foregone conclusion and production therefore would not be testimonial."); *see also Hubbell*, 530 U.S. at 30, 40–41, 44–45 (discussing "existence and location"). *But cf.* Mohan & Villasenor, *supra* note 8, at 15–16, 20 (arguing that the circuits erred in adopting a reasonable particularity standard).

[10] *In re Grand Jury Subpoena*, 383 F.3d at 910. The court notes "[t]he breadth of the subpoena . . . far exceeded the government's knowledge about the actual documents" but does not explicitly base its holding on a distinction between the actual documents and their contents. *Id.* at 910–11.

[11] *See id.* at 908, 910–11 (internal quotation marks omitted).

[12] *See id.* at 911.

[13] *Ponds*, 454 F.3d at 325.

[14] *Id.* (stating that the government knew "that the Mercedes was normally parked at [respondent's] apartment" and highlighting testimony indicating that the government knew "of [respondent's] ownership of the car" (internal quotation marks omitted)).

Under this standard method, subpoenas for the unencrypted version will typically satisfy the foregone conclusion exception. The first element—knowing the encrypted hard drive has an unencrypted version—is met through general knowledge of the encrypted hard drive's operation. When the government faces a computer with a password prompt and encryption it can't crack, the government knows there is an unencrypted version containing at least an operating system and encryption software.[15] And the second element, location, is satisfied just as plainly: the unencrypted version's "location" is the same as the encrypted computer's.

The final element, authentication, should also prove no bar. This element requires two things. First the government must have an independent authentication method[16]—a way to prove that the computer belongs to the respondent. Second, the subpoena cannot require the "use [of] discretion in selecting and assembling the responsive documents."[17]

Both these requirements are met with subpoenas that force decryption. Computers and their files can be authenticated through circumstantial evidence—that the computer was found in the respondent's home and was digitally named to include the respondent's actual name.[18] Authentication may also be proved by the respondent's own voluntary statements or the statements of others.[19]

Additionally, producing the unencrypted version of an encrypted hard drive does not require the respondent's discretion in selecting and assembling responsive documents. The government's demand for the unencrypted version tells the respondent exactly what needs to be produced: the unencrypted version of the encrypted hard drive and nothing else. The respondent does not search through his files to determine which documents are responsive and which aren't; he just finds his computer and enters his password.[20]

[15] *See* SYMANTEC, HOW ENDPOINT ENCRYPTION WORKS 1–2 (2012), http://www.symantec.com/content/en/us/enterprise/white_papers/how-endpoint-encryption-works_WP_21275920.pdf (describing how endpoint encryption works).

[16] *See* FED. R. EVID. 901(a).

[17] *In re Grand Jury Subpoena*, 383 F.3d at 912.

[18] *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012). *But cf. In re* The Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. Apr. 19, 2013), ECF No. 3, *available at* http://www.wired.com/images_blogs/threatlevel/2013/04/encryption-case.pdf (finding authentication not met on these facts), *overruled by* No. 13-M-449 (E.D. Wis. May 21, 2013), ECF No. 6, *available at* http://ia801700.us.archive.org/6/items/gov.uscourts.wied.63043/gov.uscourts.wied.63043.6.0.pdf (finding authentication met on similar facts).

[19] *See Fricosu*, 841 F. Supp. at 1237; *see also* Massachusetts v. Gelfgatt, 11 N.E.3d 605, 615–16 (Mass. 2014). *See generally* FED. R. EVID. 901(a) (allowing evidence to be authenticated by the "Testimony of a Witness with Knowledge").

[20] *Cf.* Sallah v. Worldwide Clearing LLC, 855 F. Supp. 2d 1364, 1373 (S.D. Fla. 2012) ("[T]he Court finds that [the document demands] call for objectively determinable universes of documents and do not require [the respondent] to employ the 'contents of her mind' to choose what

II.
THE SHIFT AND WHY IT'S WRONG

So that's the argument for why forced decryption is constitutional. But how has this argument fared?

Courts ruling on this issue have not engaged the argument. Some courts applied the foregone conclusion analysis to the subpoenaed item—the unencrypted version of an encrypted hard drive—and found a foregone conclusion exists, without ever saying why the inquiry should target the unencrypted version.[21] Other courts did the opposite. Facing a subpoena for the unencrypted version, they shifted the inquiry from knowledge of that version, to knowledge of "a certain file . . . ."[22] These courts, as well, never justified their approach.

A recent Massachusetts Supreme Court opinion epitomizes the lack of engagement on this issue. There, the majority targeted the unencrypted version and found a foregone conclusion existed, while the dissent targeted particular files and found the opposite.[23] Neither of the opinions explained why the focus on one over the other was right.

Here's why the courts targeting the unencrypted version (rather than the particular files) are right: (1) that's what the inquiry has always targeted (my argument above), and (2) the courts shifting the inquiry have not shown *why* it should shift.

documents might be responsive to the requests. Put simply, [the respondent] need not exercise any judgment to respond to the requests." (internal brackets omitted)).

[21] *See Fricosu*, 841 F. Supp. 2d at 1234–35, 1237 (holding that the government's knowledge, which was limited to "view[ing] the [computer's] whole disk encryption screen," established a foregone conclusion because "[t]here is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production"); *Gelfgatt*, 11 N.E.3d at 615–16 (finding a foregone conclusion where the government knew the defendant owned and operated the encrypted computer).

[22] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346–47, 1349 & n.28 (11th Cir. 2012) (requiring "knowledge as to the *files* on the hard drives" and as to "what . . . was hidden behind the encrypted wall"); *see also* Virginia v. Baust, No. CR14-1439 (Va. Cir. Ct. Oct. 28, 2014), *available at* http://hamptonroads.com/2014/10/police-can-require-cellphone-fingerprint-not-pass-code (requiring knowledge of the existence of an "unencrypted video recording" rather than of the unencrypted version of the encrypted hard drive).

It's unclear whether *In re Boucher* falls under this line of cases. The *Boucher* court held that a foregone conclusion existed because the "agent viewed the contents of some of the Z drive's files, and ascertained that they may consist of images or videos of child pornography." *See In re* Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2009 WL 424718, at *3–4 (D. Vt. Feb. 19, 2009). Thus, it was unnecessary for the court to decide if knowledge of the unencrypted hard drive generally, rather than specific files, sufficed. For essentially the same reason, an unpublished decision's classification is just as unclear. *See generally In re* The Decryption of a Seized Data Storage System, No. 13-M-449, ECF No. 6.

[23] *See Gelfgatt*, 11 N.E.3d at 615–16 (finding a foregone conclusion where the government knew the defendant owned and operated the encrypted computer); *id.* at 621–26 (Lenk, J., dissenting) (requiring knowledge of "a certain file").

Shifting the inquiry without stating reasons, of course, does not mean no reasons exist. Five possibilities come to mind: different doctrinal interpretations, functionalism, overbreadth concerns, technological misunderstandings, and metaphysical issues. But these reasons neither compel a shift nor counsel in favor of it.

1. Doctrinal Interpretations

One potential reason for the shift derives from different doctrinal readings of the same Supreme Court decision. In *Fisher v. United States*, the Court wrote that a foregone conclusion exists where production "adds little or nothing to the sum total of the Government's information . . . ."[24] With encrypted data, the government typically knows of few computer files, so producing the unencrypted version adds a lot to the government's information. So, under *Fisher*, there's no foregone conclusion.

But *Fisher* also says things cutting against this. Elsewhere the Court wrote that a foregone conclusion exists where the "question is not of testimony but of surrender."[25] Meaning, if the sought production requires "compelling a person to engage in conduct" (such as providing a voice or handwriting sample, or producing a key known to exist), there is minimal mental effort and the production is not "sufficiently testimonial for purposes of the privilege."[26] Forced decryption involves surrender, not testimony, because it compels only conduct—entering a password and turning over the unencrypted version of an encrypted hard drive.[27] Sure, that physical conduct also involves some mental effort in recalling the password. But that effort is no different from recalling a

[24] Fisher v. United States, 425 U.S. 391, 411 (1976); *In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).

[25] *Fisher*, 425 U.S. at 411; *In re Grand Jury Subpoena*, 383 F.3d at 910.

[26] *See* United States v. Hubbell, 530 U.S. 27, 34–35, 43 (2000) (first quotation) (writing of "the settled proposition that a person may be required to produce specific documents" and of "surrender[ing] the key to a strongbox"); *Fisher*, 425 U.S. at 411 (last quotation); *see also* United States v. Ponds, 454 F.3d 313, 325 (D.C. Cir. 2006) ("Because the government already had sufficient knowledge about the . . . documents, [the respondent] was simply surrendering them, not testifying, by complying with those demands in the subpoena."); United States v. MacKey, 647 F.2d 898, 900 (9th Cir. 1981) (per curiam) ("The compelled production of a physical object, such as a document, does not implicate the Fifth Amendment unless it is the act of production itself which is to be used as incriminating evidence."); *In re* Schick, 215 B.R. 4, 10 (Bankr. S.D.N.Y. 1997) ("As a [general] rule, the surrender of property of the estate is not testimonial, and hence, does not implicate Fifth Amendment concerns."). Note that some of these cited cases predate *Hubbell*, so they are not good law to the extent they contradict that decision. *See Hubbell,* 530 U.S. at 35 (holding that forcing a person to search eleven broad categories of documents and ultimately produce 13,000 responsive pages is testimonial).

[27] *See* Terzian, *The Fifth Amendment*, *supra* note 4, at 310; Terzian, *Forced Decryption*, *supra* note 4, at 60.

document's location or how to write, both of which require little thought and can be forcibly produced.[28]

What's more, post-*Fisher* cases clarify that a foregone conclusion exists even when the production adds to the government's knowledge. So long as the government has sufficient "knowledge of the existence and possession of the actual [subpoenaed] documents, not the information contained therein," a foregone conclusion exists and production can be compelled.[29] Thus, when the government subpoenas the encrypted hard drive's unencrypted version, the government need only know that the unencrypted version exists.[30] Knowledge of its particular files is irrelevant because that's the information contained in the unencrypted version.[31]

2. *Functionalism*

Another reason for the shift may be a functionalist interpretation of the foregone conclusion doctrine. Subpoenas for unencrypted versions really just hope to find particular incriminating files (e.g., child porn), so arguably the foregone conclusion inquiry should target those files.[32]

This argument has some appeal. Until computers, the government subpoenaed documents because it sought those documents. Now, with hard drives, the government isn't technically demanding documents; it's demanding containers of documents.[33] Thus there's a disconnect between what the government is subpoenaing (containers) and what it is actually seeking (certain files).

The problem with functionalist arguments, here, is that they're functionalist. Such arguments have already been rejected, so why should new ones fare better? Consider the Court's stance on the forced production of unlocking mechanisms. The government may compel the production of a

[28] *See* Terzian, *The Fifth Amendment*, *supra* note 4, at 310; Terzian, *Forced Decryption*, *supra* note 4, at 58, 60.

[29] *See In re Grand Jury Subpoena*, 383 F.3d at 910–11.

[30] *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (taking this position).

[31] *See id.*

[32] The Eleventh Circuit hinted at its functionalist motivations in its discussion of the key-combination analogy, but not in its discussion of the foregone conclusion doctrine. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) ("In *Fisher*, where the analogy was born, and again in *Hubbell*, the Government never sought the 'key' or the 'combination' to the safe for its own sake; rather, the Government sought the files being withheld, just as the Government does here.").

[33] *Cf.* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 299–300 (2005) ("In many cases, computer hardware is merely a storage device for evidence rather than evidence itself. The evidence is the electronic file that the police are looking for and that just happens to be stored along with many innocuous files inside the container of the computer hardware.").

strongbox key, but not a safe combination.[34] These are demands for essentially the same thing—an unlocking mechanism—so a functionalist approach would treat them the same. But that's not the approach the Court took. And since the Court has already rejected functionalism here, new functionalist arguments hold only so much water.

Whatever the worth of functionalist arguments, the above is not the only one. Another cuts in favor of finding a foregone conclusion. This argument, essentially, seeks parity.[35] Before computers, the government's search warrant for child porn yielded print photos.[36] Now that warrant may yield only a password prompt.[37] Print and digital photos are essentially the same thing, so the government should get digital photos just as it got print ones.

3. Overbreadth Concerns

A third reason for the shift is the potential overbreadth of digital searches. Under the Fourth Amendment, many have argued that the government is getting more evidence in digital searches than it should be—not just the items in the warrant, but also everything the government comes across while searching the computer due to the plain view exception.[38] (This exception, basically, allows the government to seize any apparently incriminating document that it sees in the course of its lawful search.[39]) In turn, at least one person has used this plain view problem to justify barring forced decryption.[40]

[34] United States v. Hubbell, 530 U.S. 27, 43 (2000) ("The assembly of those documents [the production of which requires substantial mental effort] was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to strongbox."); Doe v. United States, 487 U.S. 201, 210 n.9 (1988).

[35] Or, more precisely, it seeks to maintain the ex ante equilibrium of government power and individual privacy. *See* Terzian, *Forced Decryption*, *supra* note 4, at 56, 60–63; *see also* Terzian, *The Fifth Amendment*, *supra* note 4, at 306–11.

[36] *See* Terzian, *The Fifth Amendment*, *supra* note 4, at 300; Terzian, *Forced Decryption*, *supra* note 4, at 62–63.

[37] *See* Terzian, *The Fifth Amendment*, *supra* note 4, at 300; Terzian, *Forced Decryption*, *supra* note 4, at 62–63.

[38] *See, e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569, 576–77 (2005) ("A search for one type of digital evidence often reveals a tremendous amount of other evidence: a great deal comes into plain view."); *see also* Horton v. California, 496 U.S. 128, 133–37 (1990) (discussing the plain view exception).

[39] *See* OFF. OF LEGAL EDUC., OFF. FOR U.S. ATT'YS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 33–37 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; *see also Horton*, 496 U.S. at 136–37.

[40] *See* Erica Fruiterman, Comment, *Upgrading the Fifth Amendment: New Standards for Protecting Encryption Passwords*, 85 TEMP. L. REV. 655, 683–85 (2013) ("Given the decreased protection digital files receive under the Fourth Amendment warrant requirements, those requirements are not a sufficient substitute for robust Fifth Amendment protection of the facts that may be communicated by decryption."); *see also id.* at 681–82 (arguing that the "foregone conclusion exception should not be available in cases of compelled decryption," or alternatively, the exception should require knowledge of particular files).

But tweaking the Fifth Amendment is not the answer to a Fourth Amendment problem. If the concern is that the government is getting too much digital evidence under the plain view exception, then the fix should be fortifying the Fourth Amendment, not fortifying the Fifth. And that is exactly what some courts have done.[41]

4. *Technological Misunderstanding*

A fourth reason is based on a technological misunderstanding, and it appears in one forced decryption decision. That court believed it possible for the unencrypted version of an encrypted computer to not contain *any* files, noting that "[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives . . . ."[42] This is fatal to finding a foregone conclusion. If the government doesn't know of a single file on the unencrypted version—not even the presence of encryption software—it arguably doesn't even know if the unencrypted version exists.

But this argument's factual premise is wrong. An encrypted computer possessing a password prompt, which the computer in the above decision had,[43] must contain some files—at the very least an operating system to display that password prompt and software to encrypt the drive.[44] So, contrary to that court's conclusion, the government always knows that an encrypted hard drive has unencrypted files.

5. *Metaphysical Existence*

The final reason potentially justifying the shift is a metaphysical dispute over what it means for a document to "exist" under the foregone conclusion doctrine's first requirement. The Electronic Frontier Foundation has argued that, technically, unencrypted files do not exist on an encrypted computer.[45] In its view, only encrypted files exist, and "decryption creates new files" because "it transforms pre-existing, scrambled data into data that can be understood."[46]

But limiting existence to this technical definition doesn't mesh with how we typically define it. Say you encrypt a memo on your computer and your

[41] *See* OFF. OF LEGAL EDUC., *supra* note 39, at 36–37; Kerr, *supra* note 38, at 576–84 (discussing "three possible ways of narrowing the plain view doctrine for digital searches"); *see also* United States v. Carey, 172 F.3d 1268, 1273–75 (10th Cir. 1999) (effectively treating each opened computer file as a separate closed container).

[42] *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346–47 (11th Cir. 2012) ("The Government has not shown, however, that the drives *actually* contain any files . . . .").

[43] *See id.* at 1340, 1346 (discussing attempts to use a password to decrypt the drive).

[44] *Cf.* SYMANTEC, *supra* note 15, at 1–2.

[45] *See* Brief for ACLU Found. et al. as Amici Curiae Supporting Defendant-Appellee, at 33–34, Massachusetts v. Gelfgatt, 11 N.E.3d 605, 615–16 (Mass. 2014) (No. SJC-11358), *available at* https://www.eff.org/files/2013/10/29/brief_of_amici_curiae_aclum_aclu_eff.pdf.

[46] *Id.*

partner asks for a copy. You wouldn't respond, "The memo doesn't exist right now; give me a minute to create it." You'd just give him the memo.

The EFF's argument also proves too much. Scores of companies now encrypt their data.[47] In the EFF's alternate universe, these companies are effectively immune from discovery and subpoenas. They'd never produce unencrypted documents—they don't exist, remember—and at most they'd produce the unreadable encrypted files. I can't imagine this alternate universe becoming ours.[48]

CONCLUSION

Close readers will notice two[49] shortfalls in my argument. For one, my response to the reasons for shifting the inquiry provided only a counter, not a knockout. And I never explained why, normatively, the standard method should prevail over the shifted one.

These omissions were intentional. I've addressed both before and have nothing left to say. Plus I didn't want to detract from this Essay's main aim: tilling soil previously thought barren.[50]

Nevertheless, my argument for the standard method dovetails with my arguments elsewhere.[51] Because the Fifth Amendment seeks to maintain an equilibrium balance of individual rights and government power, and because maintaining that equilibrium requires finding forced decryption constitutional, courts should adopt any theoretically possible interpretation that permits forced decryption.

[47] *See* PONEMON INST., 2012 GLOBAL ENCRYPTION TRENDS STUDY 4, 7–9 (2013), *available at* http://www.verisec.com/sv/wp-content/uploads/sites/2/2013/03/Global-Encryption-Trends-Study-eng-ar.pdf (providing graphs and charts that show extensive, growing use of encryption technologies); *cf.* Dan Kaplan, *Thirty-Five Percent of Companies Opt Not to Use Encryption*, SC MAG. (Mar. 19, 2013), http://www.scmagazine.com/thirty-five-percent-of-companies-opt-not-to-use-encryption/article/285090.

[48] At least one court has held that, when producing encrypted documents, the company must also "provide any passwords to [the] encrypted documents," but it's not clear whether the documents were encrypted to begin with or encrypted only when produced. *See* United States v. Capitol Supply, Inc., 27 F. Supp. 3d 91, 98, 105 n.12 (D.D.C. 2014).

[49] Hopefully just two.

[50] *Cf.* Terzian, *The Fifth Amendment*, *supra* note 4, at 300 (implying the shifted method prevails over the standard).

[51] *See id.* at 306–12; Terzian, *Forced Decryption*, *supra* note 4, at 60–63.