ARTICLE:

A COMBINATION OR A KEY? THE FIFTH AMENDMENT AND PRIVILEGE AGAINST COMPELLED DECRYPTION

By **Hanni Fakhoury, Esq.**

As the purpose of encryption is to limit access to information, it is no surprise that it has also limited law enforcement's access to digital evidence. The government is often left with no choice but to force the owner to decrypt the data. Since owners are typically suspected of a crime, the Fifth Amendment to the U.S. Constitution, which provides no person can be compelled to testify against themself, should protect them. This article reviews the cases that have occurred to date and identifies the principles to emerge from them.

Introduction

In an increasingly digitized world, encryption is an integral security feature to protect data. Encryption uses computer code to change plain, readable information into unreadable random letters, numbers and symbols. Encryption safeguards sensitive information by only allowing this unreadable information – effectively gibberish – to be converted or deciphered into readable language through a specific code, commonly known as an 'encryption key.'

What was once considered security for the highly technical (and the slightly paranoid) is now an established part of modern technology. Apple's operating system, OS X, includes 'File Vault,' a program that allows users to encrypt the files in their home folders. Microsoft's Windows operating system has included Bitlocker Drive encryption since 2008. And information stored on-line, such as credit card or social security numbers are typically stored in an encrypted form as a means of safeguarding them from data theft.

As encryption gains widespread acceptance across the digital landscape, law enforcement investigators are beginning to encounter it in the course of searching through electronic devices suspected of containing evidence of a crime. The purpose of encryption is to prevent someone without the key from unlocking the data, and so naturally law enforcement efforts to bypass encryption by 'cracking' – that is, by guessing the password that protects the key – are routinely unsuccessful. When this happens, the only option is to seek the owner's assistance in either decrypting the device, or providing a plain text copy of the contents of the drive. Since the owners are frequently suspected of committing a crime, it comes as no surprise that many are reluctant to willingly assist investigators make a case against them. Moreover, owners have argued that the Fifth Amendment to the Constitution, which protects a person from being compelled to incriminate himself, protects them.

But what are the contours of this ancient constitutional right and this emerging technology? While the combination of numbers and letters needed to decrypt an encrypted device is often referred to as a 'key,' the United States Supreme Court has distinguished between a key and a combination. A person may be compelled to turn over a physical key, but cannot be compelled to turn over a combination he knows only in his mind.

So is compelled decryption turning over a combination

or a key? This article attempts to answer that question by looking closely at the few cases to address the issue.

A brief outline of the Fifth Amendment right against self incrimination

The Fifth Amendment to the United States Constitution contains a number of rights intended to protect the common citizen against government abuse in legal proceedings. The portion relevant here states that no person 'shall be compelled in any criminal case to be a witness against himself.'[1] This is known as the privilege against 'self incrimination,' and is intended as 'a prohibition of the use of physical or moral compulsion to extort communications' from an individual.[2]

There are two issues a court must decide when analyzing the right against self-incrimination. The first is whether the Fifth Amendment right applies. If it does, the second issue is to determine the extent of immunity necessary to protect the privilege.

Whether the Fifth Amendment applies

To be protected by the Fifth Amendment, a person needs to show three things: (1) compulsion; (2) incrimination; and (3) a testimonial communication or act.[3] Compulsion and testimony go hand in hand. The Fifth Amendment is not violated if the government sends a subpoena requesting information from documents voluntarily compiled – such as in a tax return – that has incriminating information because nothing has been compelled by the government.[4] A statement is incriminating if the answer either supports a conviction in a federal criminal case, or provides a 'link in the chain of evidence' to lead to incriminating evidence, even if the statement itself is not inculpatory.[5]

The most important – and the most disputed – aspect of the Fifth Amendment is the requirement of 'testimony.' That term refers not only to the act of speaking words from a person's mouth, but also to the act of producing documents.[6] Crucially, a person must make use of the 'contents of his own mind' to communicate a statement of fact.[7] For example, the act of producing documents could be considered 'testimony' if by producing the documents, the witness would be admitting that documents existed, were authentic, and in his possession or control.[8]

There are two ways an act of production can be deemed non-testimonial. First, if the government compels a person to do a mere physical act that does not force an individual to make use of the contents of his mind, that act is non-testimonial.[9] With this rationale, the court has found acts varied as providing the key to a safe,[10] standing in a photographic lineup,[11] proving a voice exemplar,[12] handwriting exemplar,[13] or blood sample[14] to be non-testimonial.

Second, if the government can show with 'reasonable particularity' that at the time it sought to compel production it already knew of the existence of the materials it was seeking, the Fifth Amendment is not implicated.[15] In other words, since turning over the information – emptying the contents of one's mind – would not reveal anything to the government that it did not already know, the testimony was simply a 'foregone conclusion.'[16] To the Supreme Court, 'no constitutional rights are touched' because the government was not relying on the 'truth telling' of the defendant, and therefore 'the question is not of testimony but of surrender.'[17] If a court has done this analysis and determined that the government is attempting to compel incriminating testimony, the Fifth Amendment's privilege applies.

The scope of immunity

Once determining the Fifth Amendment applies, the court must next determine whether it can craft immunity sufficient to preserve the privilege, but still provide the government with the testimony it seeks. Courts have recognized that the government has a 'right to every man's evidence' and can force a person to testify through a subpoena.[18] If the Fifth Amendment's privilege against self-incrimination was absolute and could never be defeated, it is doubtful that the government could

1 *U.S. Const. Amend. V.*
2 *Holt v. United States, 218 U.S. 245, 253 (1910).*
3 *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012) (citing United States v. Ghidoni, 732 F.2d 814, 816 (11th Cir. 1984) and United States v. Authement, 607 F.2d 1129, 1131 (5th Cir. 1979) (per curiam)).*
4 *United States v. Hubbell, 530 U.S. 27, 35-36 (2000).*
5 *Hoffman v. United States, 341 U.S. 479, 486 (1951), see also Hubbell, 530 U.S. at 38, United States v. Doe, 487 U.S. 201, 208-09 n. 6 (1988); Kastigar v. United States, 406 U.S. 441, 444-45 (1972).*
6 *Hubbell, 530 U.S. at 36.*
7 *Curcio v. United States, 354 U.S. 118, 128 (1957).*
8 *Fisher, 425 U.S. at 410.*
9 *Hubbell, 530 U.S. at 43.*
10 *Doe, 487 U.S. at 210 n. 9.*
11 *United States v. Wade, 388 U.S. 218, 222-23 (1967).*
12 *United States v. Dionisio, 410 U.S. 1, 7 (1973).*
13 *Gilbert v. California, 388 U.S. 263, 266 (1967).*
14 *Schmerber v. California, 384 U.S. 757, 765 (1966).*
15 *Fisher, 425 U.S. at 411.*
16 *Fisher, 425 U.S. at 411.*
17 *Fisher, 425 U.S. at 411 (quoting In re Harris, 221 U.S. 274, 279 (1911) (quotations omitted)).*
18 *Kastigar, 406 U.S. at 443 (citing Piemonte v. United States, 367 U.S. 556, 559 n. 2 (1961), Ullmann v. United States, 350 U.S. 422, 439 n. 15, and Brown v. Walker, 161 U.S. 591, 600 (1896)).*

ever investigate crime through the use of testimony. Thus, immunity statutes have long been a 'rational accommodation' between the Fifth Amendment privilege and the government's ability to compel individuals to testify.[19]

The federal immunity statute, 18 U.S.C. § 6002, states that if an order to testify has been given to a witness,

> ... the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case ...

In *Kastigar v. United States*, 406 U.S. 441 (1972), the Supreme Court explained that historically, any immunity granted under a statute, including 18 U.S.C. § 6002, must be 'coextensive' with the Fifth Amendment privilege.[20] That means the immunity must prohibit the government 'from the use of compelled testimony, as well as evidence derived directly and indirectly therefrom.'[21] These two forms of immunity have been described as 'use' and 'derivative use' immunity.

To review, a court must first decide whether the government is trying to compel incriminating testimony. If it is, the court must grant immunity that prohibits the government from not only using the words spoken or the act done against the person (typically in a trial), but also from using any other evidence obtained as a result of that testimony.

The Fifth Amendment and decryption

Turning to the issue of decryption, there are two primary questions encountered in the cases: (1) whether the act of decryption is 'testimony;' and (2) whether the government can grant immunity solely for the act of decryption while retaining the ability to use evidence found on the computer.

The cases follow the same general set of facts. The government obtains a search warrant to search a computer suspected of containing evidence of a crime.[22] Once the government possesses the computer, they are unable to search it because it is encrypted, and the government's forensic experts are unable to 'crack' it. The government's only option is to go to the computer's owner and request they decrypt the computer, or provide a copy of the computer's contents in plain text. Under these set of facts, there is both compulsion and incrimination. Generally, the individual has chosen not to help, leaving the government to go to court and request judicial intervention by ordering the person to decrypt.[23] There is also incrimination. In the three cases discussed, the individuals were suspected of a variety of crimes, including one individual already under indictment at the time of the government's request.[24]

The difficult issue then, is whether the act of decryption is testimonial, and if so, the extent of immunity to be granted. It is important to note that the issue of 'testimony' in the decryption context is not about whether the decrypted contents of the computers – the files – are 'testimonial' under the Fifth Amendment. As explained above, despite whatever incriminating character the files may have, the creation of the documents were not 'compelled' since the government did not force the defendant to create them.[25] Rather the issue is whether the act of decrypting the computer, or producing a decrypted version of the information, is 'testimonial' under the Fifth Amendment. And if it is 'testimonial,' the degree of immunity required to satisfy the Fifth Amendment.

In re Grand Jury Subpoena to Sebastien Boucher, 2009 WL 424718 (D.Vt. 2009)

Boucher approached the United States border from Canada near Vermont. Border agents saw a laptop computer in the back seat of the car, which Boucher admitted was his. An agent decided to inspect the computer and found approximately 40,000 photographs on it.[26] The images included both adult and child pornography.[27] After Boucher waived his *Miranda* rights, he agreed to speak to the agents and opened files on the 'Z drive' on the computers at the officers' request. After viewing more images and videos of child pornography in the 'Z drive,' the agents arrested Boucher and confiscated his laptop. Later, agents obtained a search warrant. While

19 *Kastigar, 406 U.S. at 446.*
20 *Kastigar, 406 U.S. at 449 (citing Murphy v. Waterfront Comm' n, 378 U.S. 52, 54, 78, (1964); Counselman v. Hitchcock, 142 U.S. 547, 585 (1892)).*
21 *Kastigar, 406 U.S. at 453.*
22 *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1339-40 (hereinafter In re Grand Jury Subpoena); United States v. Fricosu, 2012 WL 182121 *2-3 (D. Colo. 2012); In re Grand Jury Subpoena to Sebastien Boucher, 2009 WL 424718 *2 (D.Vt. 2009) (hereinafter Boucher).*
23 *See In re Grand Jury Subpoena, 670 F.3d at 1339 (government request for grand jury subpoena), Fricosu, 2009 WL 424718 at *2 (government request for order under All Writs Act, 28 U.S.C. 2651); Boucher, 2009 WL 424718 at *2 (government request for grand jury subpoena).*
24 *See In re Grand Jury Subpoena, 670 F.3d at 1339 (suspected of possessing child pornography); Boucher, 2009 WL 424718 at *2 (suspected of possessing child pornography); Fricosu, 2009 WL 424718 at *2 (indicted for mortgage fraud).*
25 *See Hubbell, 530 U.S. at 43.*
26 *Boucher, 2009 WL 424718 at *1.*
27 *Boucher, 2009 WL 424718 at *2.*

creating a mirror image of the contents of the laptop, they discovered that the 'Z drive' from which Boucher had previously opened files for the officers was encrypted. As a result, the officers were unable to take a mirror copy of the contents of the 'Z drive.' The federal government convened a grand jury, which issued a subpoena initially directing Boucher to provide the password to the authorities. After a magistrate judge found[28] the act of disclosing the password would reveal the contents of Boucher's mind in violation of the Fifth Amendment, the grand jury narrowed its request to require Boucher to provide the unencrypted contents of the computer instead.[29] Boucher challenged this as a violation of his Fifth Amendment right against forced incrimination.[30]

The trial court disagreed. It found the 'foregone conclusion' doctrine rendered the act of producing the decrypted contents of the computer non-testimonial.[31] The government knew of the existence and location of the files since Boucher had showed them to the officers personally. Nor did the order compel Boucher to authenticate the contents of the computer, since he had already done so by admitting the laptop was his and showing officers files and folders on it.[32] Thus, providing access again did 'little or nothing to the sum total of the Government's information.'[33] It did not matter that Boucher had not shown the officers the *entire contents* of the Z drive. Under Second Circuit precedent, the government was not required to be aware of the incriminatory contents of the files, just that it knew of the existence and location of 'subpoenaed documents.'[34] The court ordered Boucher to provide the government with the decrypted contents of the computer, but prohibited the government from using the act of production to authenticate the files in court.[35]

United States v. Fricosu, 2012 WL 182121 (D. Colo. 2012)[36]

FBI agents executed a search warrant at the home of Ramona Fricosu, seizing a number of computers.[37] One of the laptops found in Fricosu's bedroom was encrypted, and identified itself as 'RS.WORKGROUP.Ramona' on the whole disk encryption screen.[38] At the time of the search, Fricosu's ex-husband and co-defendant was incarcerated on unrelated charges. The day after the search, Fricosu's husband spoke to her over the telephone from prison.[39] The telephone call was recorded and included Fricosu telling her ex-husband 'they will have to ask for my help,' 'can they get past what they need to get past to get to it,' and 'my lawyer said I'm not obligated by law to give them any passwords or anything they need to figure things out for themselves.'[40] The FBI was unable to decrypt the laptop and sought to compel Fricosu to provide the unencrypted contents of the computer. Fricosu objected, claiming her Fifth Amendment right against self-incrimination would be lost.

The trial court, acknowledging the 'small universe' of cases involving the Fifth Amendment and decryption, followed the decision in Boucher and found no Fifth Amendment violation under the 'foregone conclusion' doctrine.[41] The court found the government had conclusively proven the computer belonged to Fricosu on the basis of where it was found in the house, its identification as 'RS.WORKGROUP.Ramona,' and the comments Fricosu made on the telephone to her ex-husband.[42] The court granted Fricosu immunity on the act of producing the unencrypted contents of the computer, but did not prohibit the government from using the files found on the computer against her.[43]

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012)[44]

Law enforcement officials were investigating an individual suspected of distributing child pornography.[45] Investigators were able to determine the IP addresses the suspect used to upload images and ultimately identified a specific individual, referred to as 'John Doe' in the opinion. Officers obtained a search warrant to search a hotel room Doe was staying in and seized two laptops and five

28 *See In re Grand Jury Subpoena to Boucher, 2007 WL 4246473 (D.Vt. 2007). The magistrate held forcing Boucher to decrypt would violate his Fifth Amendment right to not incriminate himself. The government appealed that decision, and the district court judge ultimately agreed with the government, reversing the magistrate. See Boucher, 2009 WL 424718 at *1.*
29 *Boucher, 2009 WL 424718 at 2.*
30 *Boucher, 2009 WL 424718 at *2.*
31 *Boucher, 2009 WL 424718 at *3.*
32 *Boucher, 2009 WL 424718 at *4.*
33 *Boucher, 2009 WL 424718 at *3 (quoting Fisher, 425 U.S. at 41) (quotations omitted).*
34 *Boucher, 2009 WL 424718 at *3 (quoting In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992 (United States v. Doe), 1 F.3d 87, 93 (2d Cir. 1993) (quotations omitted)).*
35 *Boucher, 2009 WL 424718 at *4.*
36 *In the interest of full disclosure, the author co-wrote an amicus brief on behalf of the Electronic Frontier Foundation in support of Fricosu's challenge to compelled decryption.*
37 *Fricosu, 2012 WL 182121 at *1.*
38 *Fricosu, 2012 WL 182121 at *1.*
39 *Fricosu, 2012 WL 182121 at *2.*
40 *Fricosu, 2012 WL 182121 at *2.*
41 *Fricosu, 2012 WL 182121 at *2.*
42 *Fricosu, 2012 WL 182121 at *4.*
43 *Fricosu, 2012 WL 182121 at *5. After the judge ordered Fricosu to provide the decrypted contents of the computer, the government was able to decrypt the computer without her assistance when the co-defendant agreed to decrypt the computer instead.*
44 *In the interest of full disclosure, the author co-wrote an amicus brief on behalf of the Electronic Frontier Foundation in support of Doe's attempt to not decrypt.*
45 *In re Grand Jury Subpoena, 670 F.3d at 1339.*

The court also found that the government had failed to show that the testimony was a ' foregone conclusion,' noting that there was nothing in the record that revealed the government knew whether files existed on the drive, where they were located, or that Doe was capable of decrypting them

external hard drives. FBI forensic examiners attempted to analyze the contents of the computers and drives, but were unable to obtain access to portions of the drives, which were encrypted.[46]

A grand jury subpoena was issued to Doe, requiring him to produce the unencrypted contents of the drives, and any data contained inside. Doe objected that compliance would violate his Fifth Amendment right against self-incrimination. Federal prosecutors offered Doe immunity for the act of decrypting the computer, but wanted to reserve the right to use any evidence it found on the computer against Doe.[47]

Doe refused to cooperate with the government, and ultimately he was brought before a judge who held a hearing on the issue. The most important testimony was that of a forensic examiner, who testified that the drives had been encrypted with 'TrueCrypt' software that could create partitions within a hard drive that makes some data inaccessible, even if other portions of the hard drive could be accessed.[48] The examiner testified he had obtained access to parts of the drives that were seized, only to find them blank with no data.[49] He also noted there could still be data on the encrypted part of the drive, but that he did not know for certain, and admitted there could be nothing on the drives.[50]

Doe argued that by decrypting the computer, the government would be getting derivative use of his immunized testimony.[51] In essence, he would be testifying that he, instead of someone else, placed the contents on the hard drive, encrypted the contents and could retrieve and examine them as he wished.[52] Notably, there was no testimony in the record that Doe could decrypt the computer or he was the only person with access to the devices.[53] The court disagreed with Doe, finding that compelling him to produce the unencrypted contents of the hard drives would not constitute the derivative use of compelled testimony, because Doe's act of decryption and production was not 'testimony.'[54] It held Doe in contempt of court for refusing to decrypt the drives, and committed him to the custody of the United States Marshal until he was released by the appellate court on 15 December 2011.

Reviewing the decision, the Eleventh Circuit Court of Appeals reversed the decision, finding that Doe's Fifth Amendment rights had been violated.[55] It found that decryption was not merely a physical act, like providing officers with a key, but rather it would force Doe to use the contents of his mind, similar to providing officers the combination to a safe.[56] It was the equivalent of Doe testifying about the knowledge and existence of incriminating files, as well as his possession, control and access to the encrypted drives and the ability to decrypt.[57]

The court also found that the government had failed to show that the testimony was a 'foregone conclusion,' noting that there was nothing in the record that revealed the government knew whether files existed on the drive, where they were located, or that Doe was capable of decrypting them.[58] It rejected the government's suggestion that the fact the drives were encrypted meant Doe was trying to hide something. It noted '[j]ust as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all.'[59]

Critically, it provided guidance about the showing the government must make to carry its burden under the 'foregone conclusion' doctrine:

> 'if the Government is unaware of a particular file name, it still must show with some reasonable particularity that it seeks a certain file and is aware, based on other

46 *In re Grand Jury Subpoena, 670 F.3d at 1339.*
47 *In re Grand Jury Subpoena, 670 F.3d at 1339.*
48 *In re Grand Jury Subpoena, 670 F.3d at 1340.*
49 *In re Grand Jury Subpoena, 670 F.3d at 1340 n. 10.*
50 *In re Grand Jury Subpoena, 670 F.3d at 1340.*
51 *In re Grand Jury Subpoena, 670 F.3d at 1339.*
52 *In re Grand Jury Subpoena, 670 F.3d at 1339.*
53 *In re Grand Jury Subpoena, 670 F.3d at 1340 n. 9.*
54 *In re Grand Jury Subpoena, 670 F.3d at 1341.*
55 *In re Grand Jury Subpoena, 670 F.3d at 1346.*
56 *In re Grand Jury Subpoena, 670 F.3d at 1346 (citing Hubbell, 530 U.S. at 43).*
57 *In re Grand Jury Subpoena, 670 F.3d at 1346.*
58 *In re Grand Jury Subpoena, 670 F.3d at 1346-47.*
59 *In re Grand Jury Subpoena, 670 F.3d at 1347.*

> 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.'[60]

It was the knowledge 'based on other information' that distinguished the case from *Boucher* and *Fricosu*, since in those cases the government had knowledge of what was on the computer through Boucher's actions of displaying them to the officers, and with Fricosu discussing the content on the telephone call with her ex-husband that was recorded.[61] In sum, 'although 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.'[62] The government was unable to do that.

Turning to the issue of immunity, it ruled the use immunity offered Doe was insufficient, and that derivative use immunity was necessary. Noting the critical issue was 'what conduct was actually immunized and what use would the Government make of the evidence derived from such conduct in a future prosecution,' it ruled that the federal immunity statute 'clearly immunizes both the use of the testimony itself and any information derived from the testimony.'[63] That meant no evidence found on the drives could be used against Doe if he were to decrypt the drives, since any files found would be 'directly or indirectly derived from' the compelled testimony.[64]

Decrypting the principles

While it is certainly no easy task deciphering overarching principles from only three cases, principles emerge nonetheless. Beginning with the issue of whether decryption is 'testimony,' all three cases seem to recognize that the act of decryption was not a mere physical act, reminiscent of turning over a key, but rather revealed the contents of one's mind. While *Boucher* and *Fricosu* did not explicitly say this, the government in all three cases provided immunity for the act of producing the decrypted contents of the computer. As the Eleventh Circuit noted, if 'the decryption of the hard drives would not constitute testimony, one must ask, "Why did the Government seek, and the district court grant, immunity."'[65] The 'obvious' answer for the Eleventh Circuit is that 'decryption would be testimonial.'[66] The decision in *Boucher* and *Fricosu* follow this line of thought implicitly by giving use immunity from the act of production or decrypting the computers. In other words, of the two ways an act could be non-testimonial (either as a mere physical act or under the 'foregone conclusion' doctrine), the idea of decryption as a mere physical act appears to have been rejected.

The conclusion in *Boucher* and *Fricosu* that decryption would not violate the Fifth Amendment was based on the 'foregone conclusion' doctrine. If anything, the determination of whether the Fifth Amendment is violated by compelling decryption is a factually intensive one. And both *Boucher* and *Fricosu* used the facts to determine that the 'foregone conclusion' doctrine applied. The Eleventh Circuit acknowledged this when crafting its standard, requiring the government to show that the person they want to compel, possessed an authentic file that actually exists 'based on other information.'[67] In both *Boucher* and *Fricosu*, 'other information' existed. Boucher showed the agents the files himself. Fricosu discussed the files over the telephone with her ex-husband and was clearly associated with the computer. In Doe's case, the government did not have 'other information.'

Although *Boucher*'s belief that the 'foregone conclusion' controlled is compelling, *Fricosu*'s same belief is markedly less so. *Fricosu* noted there was 'little question' that the government knew of the existence and location of the computer files, but stated that the 'fact that it does not know the specific content of any specific documents is not a barrier to production.'[68] It appears the court conflated the point that the government had proven *Fricosu* had control of the computer with the government's knowledge as to the existence of documents on the computer relevant to the criminal investigation. This proof would seem unlikely to meet the Eleventh Circuit's more demanding standard, although the other information known to the government in Fricosu was enough to at least distinguish *Fricosu*'s situation from Doe's.

Turning to the issue of immunity, it seems clear that the government can only compel decryption with a promise of not just use but also derivative use immunity, prohibiting the government from using any evidence it obtains once the device is decrypted. This stems

60 *In re Grand Jury Subpoena, 670 F.3d at 1349 n. 28 (citing United States v. Norwood, 420 F.3d 888, 895–96 (8th Cir. 2005)).*
61 *In re Grand Jury Subpoena, 670 F.3d at 1348, 1349 n. 27.*
62 *In re Grand Jury Subpoena, 670 F.3d at 1349.*
63 *In re Grand Jury Subpoena, 670 F.3d at 1349-50, 1350 n. 31.*
64 *In re Grand Jury Subpoena, 670 F.3d at 1349 (citing Kastigar, 406 U.S. at 453 (quotations omitted)).*
65 *In re Grand Jury Subpoena, 670 F.3d at 1341 n. 13.*
66 *In re Grand Jury Subpoena, 670 F.3d at 1341 n. 13.*
67 *In re Grand Jury Subpoena, 670 F.3d at 1349 n. 28.*
68 *Fricosu, 2012 WL 182121 at *3 (citing Boucher, 2009 WL 424718 at *3).*

clearly from the Supreme Court's decision in *Kastigar* as well as the federal immunity statute, 18 U.S.C. § 6002. Neither *Boucher* or *Fricosu* reached this issue since the 'foregone conclusion' doctrine applied, but it appears the government has lost this dispute.

Conclusion

So it appears that compelling decryption is like revealing a combination, rather than handing over a physical key. In some cases, the government may have to make a decision. It can either attempt to compel a person to decrypt an electronic device with the understanding that it cannot use the act of decryption, or anything found on the computer against the person. Or it can continue to attempt to 'crack' the encryption itself, reserving the right to later use whatever it finds against the electronic device's owner. The government's efforts to convince a court to allow compelled decryption will be better served if it can make a strong showing through 'other information' learned through independent investigation that the files it wants are actually on the device, and the user has access to them. Similarly, encryption programs that obfuscate and hinder the government's attempts to determine whether files actually exist on the device best serve a user who wants to protect his privacy.[69]

Given the government's choice, it seems the best course is for the government to make efforts to 'crack' the decryption itself, without the user's cooperation. To be fair, it appears this is what the government's preference is, turning to compel decryption only when it has been unable to 'crack' the decryption itself. With advances in technology, the government may inevitably be able to crack decryption quicker and cheaper than before. If used properly – within the judicial constraint and supervision that comes from obtaining a search warrant – this technology can potentially create a situation that is good for everyone: the government gets all the evidence it is entitled to, and the user does not have to testify against himself.

Hanni Fakhoury is a staff attorney at the Electronic Frontier Foundation, focusing on technology and criminal law. Previously he was a federal public defender and served as a copy editor for Defending a Criminal Case (2010). Hanni is a member of the National Association of Criminal Defense Lawyers.

hanni@eff.org

http://www.eff.org

69 *Of course, that obfuscation can you get into other forms of trouble with the government, such as a charge of anticipatory obstruction of justice under 18 U.S.C. § 1519, but that is a topic for a different paper.*