

Chapter 8. Demanding decryption

Prosecutor: Did you murder your wife?

Defendant: No.

Prosecutor: Do you know the penalty for perjury?

Defendant: No, but I bet it's less than the penalty for murder!¹

As usual, Alice and Bob are crypto-communicating at their heart's content. They are conscientious crypto users, and so they do not trust key-escrow or key-recovery systems. (Bob, who is now working in a small company, only occasionally uses self-escrow for essential stored company data.) Polly is wiretapping them, as she suspects Alice of drug dealing. She is dismayed that Alice and Bob do not use key escrow – how is she now to decrypt the wiretaps? Moreover, she wants to search Alice's house and Bob's company, but she is sure to find encrypted files in their computers – and they are smart enough to use uncrackable cryptography, and not to leave keys or passwords lingering around. Polly is at her wit's end: she will have to ask Alice or Bob to decrypt the wiretaps and the files in their computers, or to hand over their keys.

Now, a demand to decrypt or to deliver keys will run into the privilege against self-incrimination. The privilege is age-old, although there is considerable lack of agreement over the bearing of the privilege. Some define it “the right of anyone ‘charged with a criminal offence’ (...) to remain silent and not to contribute to incriminating himself.” [Funke] Others, however, think the privilege has been reduced by case law to a principle that no-one can be forced by imposition of a punishment to actively contribute to his own conviction, unless the law explicitly allows it [Reijntjes, 13]. Indeed, there seems to be a trend in the judgments of both the European Court of Human Rights (in *Funke* and *Saunders*) and the US Supreme Court (in *Fisher*, *Schmerber*, *Doe I & II*, and *Braswell*) to seriously restrict the application of the privilege against self-incrimination. In the Netherlands, the Dutch Supreme Court has swayed between discerning a general privilege against self-incrimination in the spirit of the DCCP on the one hand, and asserting that there is no unconditional principle that a suspect can not in any way be obliged to cooperate in the obtaining of possibly incriminating evidence on the other hand.

So, if there is such a thing as a privilege against self-incrimination, what does it mean? Does it prohibit Polly from asking Alice or Bob to decrypt? Can the legislature create a law to require suspects to decrypt, just as suspects can be forced to give blood to traffic police or to show books to tax agents? This chapter will investigate to what extent a decryption command is compatible with current case law, whether it could be created in legislation, given the privilege against self-incrimination, and if so, what kind of enforcement would be

¹ A classic joke, according to [Kaufman, 468].

most appropriate. First, I will make some practical remarks on decryption and key delivery (8.1.1), and on storage and communication (8.1.2). Then, I will distinguish between suspects and non-suspects (8.2), corporate entities and persons (8.3), and statements and documents (8.4), in order to narrow down the situations in which the privilege against self-incrimination holds. I shall then give my view on the rationale behind the privilege against self-incrimination (8.5), in order to assess whether a decryption command to suspects is in principle compatible with the privilege (8.6). Then, I will present the three main options for enforcing such a command: penalizing a refusal to decrypt (8.7.1), penalizing crypto use to obstruct a criminal investigation (8.7.2), and using a refusal to decrypt as evidence that Alice did it (8.7.3). In the latter case, the ‘cryptographic silence’ is used to support the evidence that Alice is guilty of the alleged crime, which I shall refer to as the ‘primary offense’ (to distinguish it from the potential secondary ‘offenses’ of refusing to decrypt or using crypto to cover up a crime). I shall conclude with an assessment to what extent a decryption command meets the principles at stake in the crypto problem, and what trade-offs are at stake if a decryption command is to help Polly catch Alice (8.8).

Although the conclusion holds for the Dutch situation, I will focus on European and US case law, which define the privilege against self-incrimination. Therefore, the analysis will by and large hold for other European countries and the United States; in fact, the European and US courts seem quite close in their application of the privilege against self-incrimination.

8.1. Preliminary distinctions

8.1.1. Demanding decryption or key delivery?

If Polly asks Alice or Bob to decrypt, in order to obtain reliable evidence, Polly will have to be there when they decrypt. Otherwise, how is she to know whether an alleged plaintext corresponds to the ciphertext at stake? If she does not have the decryption key, there is no way to check the match unless she saw it happen with her own eyes. If there are many ciphertexts to be decrypted (e.g., wiretap recordings over a period of a few months), it is not convenient for Polly to attend the entire decryption process by Alice. In many ways, it is easier and more reliable for Polly to obtain the key from Alice rather than have Alice decrypt herself. The drawback, of course, of giving Polly a master or private key, is that it potentially gives her access to many more plaintexts than the ones she is authorized to retrieve – she could use it to continue to eavesdrop on Alice and Bob after the wiretap warrant has expired, or she could decrypt recordings she made before she had a warrant. As far as protecting suspects and preventing abuse by the police are concerned, it is better to ask for decryption by the suspect rather than to command delivery of keys. A good compromise would be to ask for session keys, but this may be only possible (and often impractical) with encrypted telecommunications or with privately stored files if these were encrypted with a symmetric crypto system. Another compromise is for Alice to re-encrypt the plaintext (or re-decrypt the ciphertext) before Polly’s (or the judge’s) eyes to get the corresponding ciphertext (or plaintext, respectively). There is no real way for Alice to cheat here, and so the resulting plaintext is reliable (as being the right plaintext, that is).

Although there is a difference in practicality and protection for the suspect, for the purpose of this chapter, the effects of a decryption command and the effects of a key delivery command are largely the same: the suspect has to cooperate, and the question is whether such cooperation is compatible with the privilege against self-incrimination. In this chapter, I will therefore often use the terms ‘decryption command’ and ‘demanding key delivery’ rather indiscriminately, and generally use the term ‘decryption command’ to cover both activities.

8.1.2. Decrypting stored and communicated ciphertexts

In practice, it will make a considerable difference whether Polly asks Alice to decrypt a ciphertext intercepted in a wiretap or obtained in a search. In the latter case, with *stored encrypted data*, it will generally be possible for Alice – in principle – to decrypt. After all, if she stores data on her computer, she apparently intends to make use of them at a later time, and so, it is in her own interest to be able to decrypt. Whether she uses symmetric or asymmetric crypto does not make a difference for the *principle* of decryption ability (although it may have consequences for the *likelihood* of a denial of being able to decrypt, see 8.7.1). Note that there are some ways to subvert the decryption command by decrypting to an alternative, innocent text (duress decryption, 3.1.8).

With *encrypted communications*, the ability to decrypt afterwards is less evident. For one-way communications, notable e-mail messages, Bob will usually encrypt with Alice’s public key, which implies that she can – again, in principle – decrypt the message at any later time with her private key. Depending on when and how often Alice uses her key pair, she may or may not be able to convincingly argue that she cannot decrypt (particularly older) messages; e.g., when she has revoked her public key, or when she has been using a different key for some time, or when there is no evidence that she has recently used her private key, Alice’s chances of convincing Polly that she can no more decrypt Bob’s former messages apply. (She could also argue, less convincingly, that Bob sent her messages she was not able to decrypt in the first place; maybe Bob mistook Carol’s key for Alice’s, or perhaps the message was altered during transport.) So, with one-way communications, posterior decryption is in principle possible, although it may not always be likely.

With two-way communications, however, notably with telephone traffic, the ability to decrypt an encrypted conversation after it has ended will depend on the crypto protocol used. Alice’s and Bob’s crypto phones will have to exchange a session key before each communication. If the key is exchanged by encrypting a session key with the other phone’s public key, then Polly can ask the (holder of the) recipient phone to decrypt the encrypted session key; the crypto phone may need to be specifically configured to facilitate this. However, there are also protocols (e.g., Diffie-Hellman, cf. 7.7.1) in which the session key is derived from an unrecoverable exchange or prior session key: neither Alice nor Bob can reconstruct the session key after the conversation has ended. This feature is called ‘perfect-forward secrecy’, which is being researched by a number of cryptographers. (Some cryptographers are even concocting schemes for ‘deniable encryption’: protocols in which Alice can make the ciphertext ‘look like’ an encryption of a different (innocuous) plaintext, which she may happily decrypt for Polly’s eyes [Canetti].)

I assume that in general, it will not be feasible for Alice or Bob to decrypt past conversations. In those cases in which it may be possible, Polly can seize the crypto phone

needed to decrypt, and decrypt herself; if the phone is password-protected, she may ask Alice or Bob for the password, which is similar to the case of asking Alice for the password protecting her private key. So, for the purposes of this chapter, I will concentrate on stored encrypted data and encrypted e-mail messages.

8.2. Demanding non-suspects to decrypt

Encryption by *network operators and service providers* will not be a problem: they already have an obligation to decrypt for law enforcement. According to the EU Council resolution of 17 January 1995 on the lawful interception of telecommunications, “[i]f network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/ service providers to provide intercepted communications en clair.” [96/C 329/01, requirement 3.3] The only problem, therefore, is demanding decryption from *end users*, and here we meet the privilege against self-incrimination.

The privilege against self-incrimination is codified in the ICCPR: according to article 14 paragraph 3 sub g, everyone charged with a criminal offense has the right not to be compelled to testify against himself or to confess guilty. In the United States, the Fifth Amendment protects suspects from being a witness against themselves. The ECPHR does not contain such an explicit provision, but the European Court, in the *Funke* case, has interpreted article 6 paragraph 1 of the Convention to incorporate “the right of anyone ‘charged with a criminal offence’, within the autonomous meaning of this expression in Art. 6, to remain silent and not to contribute to incriminating himself.” As these statements show, the privilege pertains only to people charged with a criminal offense (which, in the general interpretation of the European Court, means that someone has sufficient reason to infer that he is or will be a target for a criminal prosecution. The scope of the privilege, however, is wider. Although people not charged with a criminal offense can not invoke the privilege (and, consequently, have to contribute evidence), if subsequently they are charged, compelled statements can not be used as evidence later on (at least, they could not in the case of *Saunders*).

In Dutch law, people can be required to deliver seizable things to the police, but suspects can not. (Not cooperating with such a command can be punished with up to six months’ imprisonment for not complying with an official order.) Tax officials can require people to show books, and a refusal is penalized – unless they are charged with a criminal offense.² Also, in other specialized law areas, such as the Chemical Substances Act, everyone is required to cooperate with investigating officials and to provide them with information. Finally, the registered holder of a car license number is required to tell who drove the car in case of a traffic offense, unless he can reasonably infer that he is being accused of having driven himself [HR 26 October 1993].

2 The Dutch Supreme Court held that evidence obtained by commanding a suspect to deliver documents could be used in a case against him, since at the time of the command, there was not yet a criminal charge. [HR 29 October 1996]

In general, then, people *not* charged with a criminal offense can be required to cooperate in obtaining evidence, even if this potentially incriminates them. In certain cases, the evidence thus obtained can not be used in subsequent criminal proceedings, although this is restricted to testimonial statements (see 8.4).

It follows that a decryption command can also be given to people not charged with a criminal offense. In Dutch law, this power was codified in the Computer Crime Act of 1993, with the proviso that the command can not be given to a suspect.³ Compelled testimonial statements obtained in this way may not be used in subsequent criminal proceedings against the person testifying, however. Assuming for the moment that a key delivery is a privileged testimonial statement (cf. 8.4), two interesting questions can be asked in this respect.

First, can the compelled evidence be used in criminal proceedings against *other* people? Suppose Polly forced Bob to say what key he and Alice used. Since Bob is not a suspect himself, the key can be used to decrypt the wiretaps, and these can be used in a case against Alice. Even if Bob would be a suspect, and his compelled rendering of the key would violate his privilege against self-incrimination, the key might still be used against Alice anyway, as it was not she who rendered the key and it therefore did not breach *her* privilege.⁴ It seems logical that it does not violate the privilege, because it is a privilege that protects suspects against incriminating themselves – it does not protect them from incriminating statements uttered by others (otherwise, where would witnesses for the prosecution be?). Therefore, the Public Prosecutor can split multiple criminal cases, so that evidence obtained from one suspect can be used in proceedings against the others.⁵ Of course, if Alice and Bob use asymmetric encryption, Bob can only decrypt (e-mail) messages sent to him by Alice (and not the messages he himself sent to Alice, unless he kept a plaintext copy), but these are the most interesting messages. The only thing Bob cannot decrypt, of course, is the files stored on Alice's computer.⁶

A second question is whether an unlawfully compelled rendering of a key also contaminates the resulting evidence: if Alice was forced to give the key to the encrypted files

3 As the class of suspects is larger than the class of people charged with a criminal offense (although the boundary is somewhat fuzzy), for convenience's sake, I shall take the larger class (of suspects, that is) as a basis in this section. If a decryption command can not be given to a suspect, it can certainly not be given to someone charged with a criminal offense.

4 This argument holds for the Netherlands (the *Schutznorm*) as well as for the US. In *Couch v. United States*, an accountant was forced to give tax papers of his (suspect) client. This did not violate the Fifth Amendment, as no personal compulsion was used against the accused. "The Constitution explicitly prohibits compelling an accused to bear witness 'against himself': it necessarily does not proscribe incriminating statements elicited from another." The *Federal Guidelines for Searching and Seizing Computers* also suggest asking others for a crypto key or password: "Agents should consider whether the suspect or someone else will provide the password if requested. In some cases, it might be appropriate to compel a third party who may know the password (or even the suspect) to disclose it by subpoena (with limited immunity, if appropriate)." [CD, 55]

5 For this reason, it is common practice in the Netherlands to split cases against several suspects involving the same offense.

6 A problem may occur when Bob (as accomplice) wants to shield Alice. The punishment for his not complying with a decryption command (a regular three months, in the Netherlands), will in that case not be a strong encouragement for him to cooperate. See further 8.7 on this problem.

on her computer, is it only the key which cannot be used as evidence in court, or also the files decrypted with this key? The ‘fruits of the poisoned tree’ doctrine tells that evidence resulting from an illegal investigation activity can not be used as evidence in court.⁷ In general, if a key delivery is privileged, then also the resultant plaintexts will be protected by the privilege.

A first conclusion is that the police can require non-suspect people to decrypt.⁸ If a key delivery is a privileged testimony, the key (and generally the data decrypted with that key) can not be used as evidence in subsequent criminal proceedings against the person who rendered it; however, they may be used in proceedings against others. This can be useful in many cases, since it means that encryption by non-criminals will not hamper an investigation. Thus, for instance, if the police is authorized to demand data from banks, accountants, or notaries, the data will have to be provided in plaintext. Also, the police can require crypto service providers, in particular Key Escrow Agents and Data Recovery Agencies, to decrypt or to hand over keys; this may be possible mainly in business crime cases, if the corporation uses a data-recovery service.

8.3. Demanding suspect corporations to decrypt

Suppose Polly suspects Bob’s company of tax fraud, and she wants to search the company and investigate Bob’s computer. Can she ask Bob to decrypt files she finds there? In principle, corporate entities can claim constitutional rights protection. Can Bob’s company benefit from the privilege against self-incrimination? The European Court of Justice decided in the case of the French enterprise *Orkem* that the European Commission “may not compel an undertaking to provide it with answers which might involve an admission on its part of the existence of an infringement [anti-competitive conduct] which it is incumbent upon the Commission to prove.” Although this recognizes that enterprises do have a privilege against self-incrimination,⁹ it restricts its application to an *admission* of the *existence* of an *infringement* – that is, a virtual confession. Requiring the handing over of corporate records could well be admissible, since this would not admit the existence of an offense – only of books that an investigation agent knows the enterprise must have anyway.¹⁰ Therefore, asking the self-escrow agent within Bob’s company to hand over the keys (or plaintexts) will be possible, as it is clear that he must have the keys (or plaintexts) available as corporate records.

7 It is possible that, having cunningly obtained the key from Alice, the police claims that in the meantime they had been running an exhaustive key search, and that it just so happened they were very lucky and ‘found the key’ in the first batch of trials. The unlikelihood of such a lucky find depends on the strength of the crypto system; in many cases, the judge may do away with such a claim and conclude that Polly has used a key she unlawfully obtained from Alice.

8 They can also require suspects not (yet) charged with a criminal offense to decrypt.

9 This is not so in the United States: “the corporation (...) of course possesses no such privilege.” [Braswell]

10 The Dutch Supreme Court ruled that a command to deliver accounting evidence can also be given to suspects. [HR 29 October 1996]

Then, one should ask whether Bob himself can be called upon to decrypt. In the United States, the protection of the Fifth Amendment for persons working in corporate entities has been reduced severely. Notably in *Braswell*, the Supreme Court said that corporations cannot claim protection by the Fifth Amendment when people are required to hand over corporate records. Even if the handing over can be seen as an admission of their existence, “a custodian may not resist a subpoena for corporate records on Fifth Amendment grounds.” One reason for deciding so, is a political one: “The greater portion of evidence of wrongdoing by an organization or its representatives is usually found in the official records and documents of that organization. Were the cloak of the privilege to be thrown around these impersonal records and documents, effective enforcement of many federal and state laws would be impossible.”¹¹ This indicates two considerations: the records required are corporate, which means their existence is presupposed, and there is no claim for personal privacy for corporate records. That means that employees of a company can be forced to give these documents. Only if the employee ‘is’ the company himself, can he invoke the privilege: in *Doe I*, the privilege against self-incrimination could be invoked because Doe conducted his business as a sole proprietorship, and therefore acted in a personal rather than a representative capacity (and because the act of production (not the contents) was a testimonial self-incrimination). *Braswell*, on the other hand, was co-director, and hence subject to the ‘collective entity rule’, which treats corporations different from individuals. The European situation is similar in this respect, although there may be more constitutional protection in Europe and the Netherlands for employers if they can be held personally (criminally) liable for corporate offenses.

One can conclude that in Europe, employees and employers of an enterprise can only claim protection from self-incrimination if the compelled production of evidence (the *act of producing*, not the evidence) directly admits guilt to having committed an offense, or if the documents (or statements) required are private and outside the scope of the corporation. In the United States, there is no privilege for corporations, nor is there for custodians of corporate records, except when the enterprise is conducted as a sole proprietorship and the act of production is testimonial self-incrimination.

In the case of Bob and his enterprise, handing over a key cannot be supposed to be an admission of the existence of an offense. There may be a problem if the files decrypted with the compelled key turn out to be private, say, e-mail messages from Alice asking for XTC pills. In that case, one can argue that the resulting decryptations can not be used in a case against Bob (for complicity in drug dealing); as in this case, Polly was interested in tax fraud by Bob’s company, this need not be a significant drawback. The main thing is that Polly can require Bob to decrypt corporate files, except when Bob conducts his business as a sole proprietorship (US) or is an executive who can be held criminally liable for corporate offenses (Europe), and the act of production would be a testimonial self-incrimination.

11 The Dutch Supreme Court, in its 29 October 1996 verdict, likewise acknowledged that the legislature can create a power to command a suspect to cooperate in specific (law) areas, given the concerns relating to the enforcement of the pertinent criminal provisions, and the special demands and problems of finding the truth in such cases.

8.4. Demanding individual suspects to decrypt

Asking whether Polly can command suspect Alice to decrypt or to hand over the key, is asking the sixty-four thousand dollar question: what kind of (possibly incriminating) compelled cooperation is compatible with the privilege against self-incrimination? The key issue here is whether the privilege concerns only oral testimony or extends also to other forms of cooperation, such as handing over keys or documents.

Dutch penal legislation seems to incline (with a few exceptions proving the rule) to a broad interpretation of the privilege, and prevent the compelled rendering of documents by suspects. The command to hand over seizable goods cannot be given to suspects (art. 107 para. 1 DCCP), nor can the command to provide law enforcement with data (art. 125m para. 1 DCCP). One exception is a specific provision enabling investigating officers to command delivery of goods for a number of specific crimes (art. 551 para. 1 DCCP), which does not refer to privileged suspects, and the Dutch Supreme Court has allowed such a command to be given to a suspect [HR 20 March 1984].¹²

The European and US courts appear to apply the privilege in a more restricted sense, covering only factual testimony. For Europe, the verdict of the ECHR in *Saunders v. United Kingdom* is paramount. Saunders had been compelled to testify during an administrative investigation into an alleged corporate fraud. His statements were subsequently used during a criminal trial against him, in a manner which sought to incriminate him (by calling into question his honesty and casting doubt on his version of events). The European Court considered this use of compelled statements unacceptable in light of the privilege against self-incrimination. And in doing so, it virtually restricted the privilege to using incriminating *statements*: the privilege “is primarily concerned, however, with respecting the will of an accused person to remain silent. (...) it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, *inter alia*, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing.”

The European Court had earlier called the rationale of the privilege against self-incrimination, among others, protecting the accused against improper compulsion by the police, which contributes to avoiding miscarriages of justice and to securing the aims of article 6 of the Convention [Murray, at 45]. Compelled statements may be unreliable – who knows what someone will say in fear of violence or punishment? – and miscarry justice, but a suspect cannot lie with blood or documents (that is, documents which exist at the time of the command, and which the suspect has no ability to alter).

This view of the privilege is the key to interpreting an earlier case which had caused some confusion with ECHR watchers. *Funke* was compelled by French customs officers to render bank statements of foreign accounts. The European Court considered this a violation “of the

12 Article 551 paragraph 1 DCCP concerns a few specific crimes, such as those involving state security, migrant trafficking, child pornography, cruelty to animals, and certain offenses against public decency; in these cases, a delivery command can be given to suspects.

right of anyone to remain silent and not to contribute to incriminating himself.” This phrasing suggested the Court maintained a broad view of the scope of the privilege against self-incrimination: no suspect is required to contribute to incriminating himself. This would imply that many laws forcing suspects to give blood or to breathe in a breathalyser test are violating the European Convention. *Saunders* sheds light on this judgment: it is not the rendering of documents *as such* that breached the privilege, it was the fact that the officers were not sure that the documents required *existed at all*, and so, the rendering of the documents was in effect an admission by Funke that he possessed them. One can read this between the lines of the Court’s phrasing of the action: “the customs secured Mr Funke’s conviction [for his initial refusal to give the bank statements] in order to obtain certain documents which they *believed* must exist, *although they were not certain of the fact.*” [emphasis added] The police can command a suspect to hand over documents, but, like with blood, they must know the documents exist and that the suspect has them at his disposal.¹³ Otherwise, his refusal to give them can mean two things: he does not have them, or he does not want to give them; in other words, a refusal does not give reliable evidence – you cannot draw conclusions from it.

The view that suspects can be compelled to deliver documents can also be seen in recent US Supreme Court judgments. In *Fisher v. United States*, Fisher’s attorney was subpoenaed to hand over tax returns drafted by Fisher’s accountant. The Court referred to *Schmerber*, where it had ruled that the privilege against self-incrimination only protects evidence of a testimonial or communicative nature (which, in that ruling, excluded furnishing a blood sample). Fisher’s tax returns did not contain compelled testimonial evidence, as they had not been drafted under compulsion. The SC remarked that under certain circumstances, handing over documents could be testimonial and incriminating, if in handing them over, the holder would admit his possession of the documents, and if his possession was not a foregone conclusion (say, because the existence and location of the documents were known to the police from other sources). In *United States v. Doe*, the Court built on this decision. Doe was commanded to hand over business documents he himself had drafted. The SC considered these documents not to be privileged through their content (he had not drafted them under compulsion), but stated that the *act of producing* them could be testimonial; in this case, it was, since “the act of production would compel respondent to ‘admit that the records exist, that they are in his possession, and that they are authentic.’”¹⁴ Whether the *contents* of a statement are testimonial in nature, was defined in *Doe II*. Doe was ordered to write an authorization for foreign banks to disclose information. According to the Court, this was not testimonial, since the authorization did not disclose factual statements. The privilege only protects a suspect from forced disclosure of ‘the contents of his own mind’; the statement (oral or written) must relate, implicitly or explicitly, a factual assertion or disclose

13 It seems the protection against self-incrimination in the United Kingdom is broader: ‘a man is not bound to provide evidence against himself by being forced to answer questions *or produce documents*’. [Reijntjes, 60]

14 Compare the ECHR *Saunders* ruling: “some of the applicant’s answers were in fact of an incriminating nature in the sense that they contained admissions to knowledge of information which tended to incriminate him”, and as such, they could not be used as evidence.

information.¹⁵ One can conclude from these verdicts that the privilege only prohibits the compelled writing or uttering of factual statements, as well as the compelled handing over of documents if this act itself admits the holder's possession, and if his control over the documents can not otherwise be proved.¹⁶

Now, this case law gives Polly some reassurance. If Alice has stored her key on a diskette or a smart card, and if Polly is certain of its existence and Alice's possession of them, she can summon Alice to deliver it – at least, in the United States she can, and also in European countries, according to the European Court's decision in *Saunders*. In the Netherlands, article 107 paragraph 1 DCCP, however, prohibits Polly from commanding delivery from suspects.¹⁷

But what if Alice has learnt her key by heart, or has stored and password-protected it, as will mostly be the case? Can Polly ask Alice for the key or password? Here, we meet the border line of the privilege: is a key or password testimonial? That is, is it part of someone's 'integrity of conscience', or is it comparable to a physical key? One can think of a cryptographic key as equivalent to a physical key to a door. There is one fundamental difference, however: the physical key exists outside of the holder's mind, and the police can – in theory – find it by searching well, even if the holder does not cooperate. The courts in that case allow a delivery command for non-testimonial evidence: if the evidence exists outside of the will of the suspect, and its existence and the suspect's possession are clear from other sources, then the police can command delivery (in a way, this is a service to the suspect, as it may save her a ravaging of the house). With a cryptographic key or password, this is different: it does not (have to) exist outside of Alice's mind, and if Alice does not give it, there is no way the police can find it. Although – theoretically, there is: an exhaustive key search. As pointed out in section 3.1.5, this is not realistic in most cases. However, the fact that there *is* an alternative to find the thing looked for, however impractical, may be an argument to convince a court that a command to give a key or password is valid. (Mark that this is, in fact, a paradoxical conclusion: you may only use a power when there are alternatives.)

Compare the distinction Judge Stevens made in his dissenting opinion in *Doe II* (note 9), essentially unchallenged by the majority: "He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe – by word or deed." The Court considered the compulsion at issue (the authorization) to be "more like be[ing] forced to surrender a key to a strongbox" than like revealing the combination to a safe. The fundamental difference seems to be that of mind versus matter: the key to a strongbox exists anyway, whereas giving a combination to a safe reveals a person's knowledge, and thus is testimonial. In that respect,

15 Judge Stevens dissented, arguing that the authorization statement was privileged, as "by executing the document, petitioner admits a state of mind, a present-tense desire." "But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. (...) The forced execution of this document differs from the forced production of physical evidence just as human beings differ from other animals." (219)

16 Another privileged act is when the handing over of documents authenticates them. [*Andresen v. Maryland*]

17 Only in the case of article 551 paragraph 1 DCCP could Polly demand delivery, which will not be possible in many crypto cases.

a safe combination is like a crypto key or password. A minor difference between a safe combination and a crypto key is that it may be easier to prove earlier knowledge of a crypto key than knowledge of a safe combination. If Alice has signed a document (very) recently with her key, which can be proven if she has a public-key certificate, this is strong evidence that she holds her private key (and remembers the password). She may claim to have just forgotten it when the police arrived, but this is rather too convenient to be convincing. I equate a crypto key or password with a safe combination rather than a strongbox key. If the police can argue that Alice holds the key or knows the password, to the extent that Alice's knowledge is a foregone conclusion, then *Doe I* suggests that a key delivery command is legal. In general, it may be a (too) hard task for the police, however, to make Alice's disposal of the key or password a foregone conclusion (compare 8.7.1). By and large, *Doe's* 'foregone conclusion' is the same requirement as *Funke's*, namely that the police must be sure of the fact that the documents exist and that the suspect has them available; therefore, this conclusion holds for both the US and Europe.

Like demanding key delivery, demanding Alice to decrypt will also often fall within the present scope of the privilege against self-incrimination. Although police agents can compel suspects to allow the taking of a blood sample or to give a writing sample, this is not giving testimonial evidence, as the integrity of conscience is unimpaired, and the evidence exists outside of the will of the suspect (handwriting is a characteristic of a person, and so she cannot intentionally falsify it, as experts can attest). Should Alice decrypt a document, then she would testify to knowledge of the key, and this is as testimonial as handing over the key or password itself.

Overall, then, Polly does not have much foothold for commanding suspects to deliver a key or to decrypt, as current case law stands. Only if she can show that Alice's knowledge of the key is a foregone conclusion, can she demand decryption.

8.5. The rationale behind the privilege against self-incrimination

Given the conclusion that, under current case law, a decryption command to a suspect will generally be obstructed by the privilege against self-incrimination, what are the options for the legislature to specifically create such a command? In drafting the 1993 Computer Crime Act, the Dutch legislature explicitly created a decryption command only for non-suspects, ostensibly respecting the privilege against self-incrimination. With the decision to withdraw the proposed article from the draft Computer Crime Act II to demand suspects to decrypt, this starting point was reinforced. In the US, federal-government computer search and seizure guidelines imply that encryption keys and passwords may be protected by the Fifth Amendment.¹⁸ However, is the privilege fundamentally contrary to a decryption command, or is it only currently considered disproportionate to allow the command to be given to

18 "In some cases, it might be appropriate to compel a third party who may know the password (or even the suspect) to disclose it by subpoena (with limited immunity, if appropriate)." [CD, 55] The 'limited immunity' indicates that the password may be privileged under the Fifth Amendment.

suspects? Would it be acceptable to somehow infringe upon the privilege against self-incrimination? As the privilege is not absolute, one may investigate its margins. This requires deeper scrutiny into the background of the privilege against self-incrimination: what is its rationale?

There are various viewpoints on the rationale of the privilege against self-incrimination. Historic interpretations tend to stress the humanity principle: “in the end, is it not the point that we think it inhumane, and so we reject this ethically, to force someone to contribute to his own misfortune? Do we not think that every citizen has to right to protect himself – even if this harms truth-finding?” [Reijntjes, 18] In a way, the privilege shields the police from being tempted to force someone to give evidence, and this protects suspects from torture and inhuman treatment.¹⁹ However, this historic explanation is not satisfactory to pinpoint the kernel of the privilege. If it is unethical to force someone to contribute to his misfortune, we should ban other forms of compelled cooperation that have gradually slipped into our legal systems, such as taking blood samples, doing line-ups, giving writing samples, or, indeed, delivering documents. Giving blood can be as devastating to a suspect as a confession of guilt, yet we allow the first while rejecting the latter. Humanity is not the all-encompassing reason of the privilege.

Others have discerned a privacy component to the privilege against self-incrimination. Notably in the US, the Fifth Amendment is often related to the Fourth, which protects people from unwarranted searches and seizures. Since the Fourth is aimed at protecting privacy of the home, the Fifth can also be seen as protecting the privacy of the mind. According to a recent decision, *Pennsylvania v. Muniz*, the Fifth Amendment privilege reflects “our respect for the inviolability of the human personality and of the right of each individual ‘to a ... private life.’” [quoted in Sergienko]²⁰ This contrasts sharply with Justice O’Connors concurring opinion in *Doe I*: “the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind.” [*Doe I*, at 618] It is hard to see that the Fifth Amendment protects the privacy of one’s mind if it does not protect the privacy of (some of) one’s papers. In European case law, there is little evidence to suggest that the privilege against self-incrimination is meant to protect suspects’ privacy. In *Murray*, the Court stated that the privilege contributes to the “avoidance of miscarriages of justice” and the securing of the aims of article 6 of the ECPHR – that is, not the goals of article 8 ECPHR on privacy. And if compelled delivery of documents the suspect was not compelled to write by the police (a diary, for instance) is compatible with the privilege against self-incrimination, there is little privacy protection in the privilege.

Another attempt at explaining the reason of the privilege has been to distinguish between passive suffering and active cooperation; several people have suggested the privilege protects only the latter. This would explain why someone can be forced to give blood, but not to

19 In *Murphy*, the Court articulated seven purposes of the privilege against self-incrimination, including “unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt” and “our fear that self-incriminating statements will be elicited by inhumane treatment and abuses”.

20 Sergienko notes: “This statement is difficult to reconcile with interpretations of the Fifth Amendment providing no protection for existing documents.”

provide a testimony. Indeed, the system of the Dutch Code of Criminal Procedure seems to suggest such a distinction: a suspect must allow his clothes or body to be searched, but he cannot be compelled to deliver goods or information. The Dutch Supreme Court has once phrased the privilege thus: the principle that a suspect – safe in exceptions provided in law – cannot be compelled to *actively* cooperate with something which can lead to his conviction [HR 1 October 1985, emphasis added]. People favoring the distinction have been forced, however, to make some distorted attempts at fitting allowable ‘passivities’ into the framework: one can, for instance, hardly define someone being forced to change clothes and to take part in a line-up as cooperating passively. More importantly, the distinction has little explicative value to pinpoint the reason behind the privilege. The Dutch Supreme Court has perhaps arrived at the same conclusion; in later case law, at least, it reverted to its general wording of the privilege, leaving out mention of ‘active’ cooperation.

In my view, there is a more plausible interpretation to the privilege against self-incrimination than humanity, privacy, or activity. Its *raison d’être*, as I already have implied in 8.4, is the *reliability* of evidence. Compelling someone to provide evidence can lead to unreliable evidence, if the suspect can alter the evidence, if he is too frightened by the imposing police to tell the truth, or if he simply does not know the answer. That is why the European Court speaks of avoiding miscarriages of justice.²¹ Schalken has argued the case for this interpretation convincingly:

“In that vision, which remains close to the text of article 14 paragraph 3 sub g ICCPR, which prohibits unwilling self-incrimination by testimonies, a compelled violation of the *freedom of statement* by the suspect is central. One can maintain that this relates to the reliability of the evidence. In that approach, it becomes visible that, as the method of finding the truth becomes less reliable, the significance of the privilege against self-incrimination increases. (...) The reverse then also holds: as the method of research yields more reliable evidence, the force of the privilege against self-incrimination decreases. In that sense, one can maintain that the principle, contrary to what is defended in the literature (...), is not incompatible with breath analysis and blood samples for drink-driving checks and DNA testing. The information which can be gained on this basis is available and unequivocal. The safeguards needed with this type of investigation are aimed at both safeguarding the meticulousness of the procedure with a view to the reliability of the evidence, and at ensuring that other principles are met, such as the principle that the finding of truth can not be served in another way and that therefore there are no reasonable alternatives (subsidiarity) and the principle that the gravity of the violation of the suspect’s rights, in particular the right to safeguarding the integrity of the body and privacy, must be proportionate to the gravity of the offense to be solved (proportionality). The concern that the constitutional and conventional rights of the suspect aim to protect must, with humanity as the lower limit, be traded off with the concern that is at stake in a violation of those rights.” [Schalken]

I consider this the most adequate description of the rhyme and reason of the privilege against self-incrimination. If the information asked from the suspect is available and unequivocal, the privilege plays no significant part. If the information is not (necessarily) available or if it can be equivocal, the privilege shields the suspect from having to give it or the judge from

21 Judge Martens, who dissented in *Saunders* because he considered the Court to interpret the privilege too broadly, concurred in this respect: “since there is a not negligible chance that statements made under pressure may be unreliable, the rationale of the immunities under discussion comprises – as the Court put it – the avoidance of miscarriages of justice.”

being able to use it as evidence.²² This is almost only the case when someone is forced to give testimonial statements. This view of the privilege takes into account the humanity principle (as a lower limit), and it explains the distinction between ‘passive’ and ‘active’ cooperation, which, in fact, is a distinction between non-cheatable and cheatable cooperation.²³ At the same time, it explains both the relative reluctance of the legislature to infringe the privilege and the relative ease of the courts to allow infringements. The legislature has so far found little occasion to create general powers that infringe the privilege, given the subsidiarity principle: they have only done this with blood samples for drunk-driving testing (after all, this is the only way to prove drunk driving, in a neutral, verifiable way), and with DNA testing for serious crimes (punishable with eight years or more) and a small number of violent crimes. The courts have restricted the scope of the principle much more in specific cases, as the circumstances of a particular case allow a much sharper application of the subsidiarity principle. In particular, material “which has an existence independent of the will of the suspect” can be obtained from a suspect through the use of compulsory powers (*Saunders*), because it is available and it can not be altered.

8.6. Is it possible to create a law demanding decryption?

Now, can a law authorizing decryption commands be compatible with the privilege against self-incrimination, if the privilege is primarily aimed at safeguarding the reliability of evidence? Let me first look at handing over a decryption key. Obviously, if Alice gives Polly ‘the’ key, it either works or it does not. If it works, i.e., if the result of decryption with the key is a reasonable plaintext, then it must be the right key. Only if Alice used a One-Time Pad (OTP) to create a dummy message, she may not hand over the right key, but a fake dummy key (see 3.1.8). If Alice decrypts with a OTP, then, it is wise for Polly to be suspicious (who, after all, uses OTPs these days?), and Alice may have to explain how she generated the key (which should be a random stream at least as long as the message itself). If Alice has prepared herself well, she may get away with it, but generally, dummy decryption will not be practical or convincing.

The evidence of the key, then, is reliable. Safe for the cumbersome option of creating dummy messages with double keys, Alice can not cheat with the key. Like blood or breath, it exists outside of her will. The same holds for a password she gives to release a key stored on a smart card or hard disk: it works or it does not. Therefore, the evidential value of a

22 Compare article 76 paragraph 2 of the English Police and Criminal Evidence Act 1984: “If, in any proceedings where the prosecution proposes to give in evidence a confession made by an accused person, it is represented to the court that the confession was or may have been obtained (...) in consequence of anything said or done which was likely, in the circumstances existing at the time, to *render unreliable* any confession which might be made by him in consequence thereof; the court shall not allow the confession to be given in evidence against him”. [emphasis added]

23 As A.J. Marx put it in 1934: “It is something very different to let words cross one’s lips, with which one incriminates oneself, than it is to cooperate in an examination that allows objective conclusions, which can equally well be in favor of the suspect as against him.” [quoted in Ansmink, 428]

Voices for demanding decryption

The option of addressing the crypto problem by giving the police the power to demand decryption, or to shift the burden of proof, has proponents in several countries.

The Delegation of *Australia* to the OECD December 1995 Ad Hoc Meeting, for instance, noted that "the law on self-incrimination may need to be reviewed", since "the person served with a search warrant requiring decryption of his or her information may, conveniently 'forget' the key." [Australia, 7] When the report was discussed at the meeting, *Denmark* "offered the observation that in some circumstances the Danish courts will shift the burden of proof to the defendant if he does not provide certain kinds of evidence that is within his control." [Baker 96] Indeed, Danish scholars Andersen and Landrock have proposed that "a principle of 'reversal of proof' should apply in cases where three conditions [are] met: first, circumstantial evidence suggests that a person is guilty of an offence. Second, there is a substantial likelihood that the defendant has encrypted information that might provide evidence of guilt. And third, the defendant is in a position to decrypt that information and thereby free himself of any allegation, but decides not to." [Andersen, 348]

The *UK* Labour Party, before governing, opposed key escrow. Instead, they said, "the only power we would wish to give to the authorities, in order to pursue a defined legitimate anti-criminal purpose, would be to enable decryption to be demanded under judicial warrant." [Labour] Two *Belgian* senators have likewise proposed such a power. To "prevent that certain people refuse to give the key or to cooperate with the judiciary," they propose heavy criminal sanctions, because "if the person does not want to hand over the key, the judiciary has no evidence whatsoever against him and he can go free." Therefore, they propose a maximum of five years' imprisonment for those who are able to assist in decryption yet refuse to do so. [Bribosia] The *Irish* framework for cryptography policy states that "legislation will be enacted to oblige users of encryption products to release, in response to a lawful authorisation, either plaintext which verifiably relates to the encrypted data in question or the keys or algorithms necessary to retrieve the plaintext. Appropriate sanctions will be put in place in respect of failure to comply." [DPE]

The *Dutch* Data Protection Authority, in a 1998 letter to the Minister of Internal Affairs, expressed its alarm at the obligation to deposit keys that the Minister was apparently (still? again?) considering. The Data Protection Authority greatly preferred the system of requiring people to decrypt, as initially proposed in the draft Computer Crime Act II. [Registratiekamer 98]

delivered key is highly reliable, and consequently, a command to deliver a key or password is, in principle, compatible with the rationale of the privilege against self-incrimination.

The same is valid, *grosso modo*, for demanding the suspect to decrypt herself. As Polly will not be satisfied with a plain message just because Alice tells her it is the plaintext of the encrypted file at issue, Alice will either have to decrypt it before Polly's eyes, or she will have to re-encrypt the plaintext (or redecrypt the ciphertext) before Polly's or the judge's eyes to get the corresponding ciphertext (or plaintext, respectively). There is no real way for Alice to cheat here (with the same proviso when she uses a One-Time Pad), and so, the resulting plaintext is reliable (as being the right plaintext, that is; the contents may still be unreliable, of course). Therefore, in principle, a command to decrypt is compatible with the privilege's rationale.

In this respect, delivering a crypto key or decryption is comparable to furnishing a blood sample or a writing sample. The difference, however, is that with the latter, it is a foregone conclusion that the suspect is *able* to comply. With delivering a key or decrypting, one can not take for granted that someone can comply.²⁴ This is, I think, the crux for generally holding that revealing a safe combination is privileged: the act shows knowledge of the combination, and this is testimonial. Only if knowledge of the combination is a foregone conclusion, then, one can argue, the privilege does not hold. If one is to explore the margins

²⁴ This, in my view, is the essence of *Funke*: if the customs officials *had* been sure of the fact of the documents' existence, they *could* have ordered their delivery. Since they were not sure, the order was unlawful.

of the privilege against self-incrimination, it is this issue that seems to be crucial. If the ability to comply is not a foregone conclusion, then the reliability of the evidence decreases – not when the suspect complies, but when she refuses. After all, a refusal can mean either inability or unwillingness, and if there are no compelling arguments that it is unwillingness, one cannot draw a conclusion from the suspect's refusal to comply. One can echo Schalken here: if there is less evidence that the suspect is able to decrypt, the significance of the privilege against self-incrimination increases; as the evidence that the suspect knows the key or password increases, the force of the privilege decreases.

Therefore, legislation granting an explicit power to demand decryption from suspects is compatible with the privilege only insofar as there is strong evidence that the suspect is able to decrypt or give the key. That is more or less the same conclusion I arrived at from examining case law: only if Polly can show that Alice's knowledge of the key is a foregone conclusion, can she demand decryption. I conclude that, in principle, creating a power to demand decryption from suspects is compatible with the privilege against self-incrimination, making explicit what is already possible under current case law (except in the Netherlands), with the condition that there must be strong or even compelling evidence that a suspect is able to comply.

8.7. How to enforce a decryption command

For a power to command decryption or key delivery to be effective, the legislature must create an incentive for the suspect to cooperate. After all, Polly can always kindly *request* Alice to decrypt – and Alice can kindly refuse to do so. If the refusal does not somehow reverberate upon Alice, she will of course not cooperate (unless to discharge herself). What kind of pressure can the legislature use to incite Alice to cooperate? There are three ways of doing so. First, penalize the refusal – just as currently a refusal to obey a legal order is punishable with up to three months' imprisonment. A second, similar, option is to penalize the use of encryption 'to obstruct an investigation', or (if there is enough evidence) to consider crypto use an aggravating circumstance, and consequently give Alice a higher sentence if she refuses to decrypt. A third method is to use the refusal to cooperate as evidence in the primary case: if Alice does not want to decrypt, she apparently has something to hide, and the encrypted file may be thought to be incriminating. This would make it easier for the judge to convict Alice given an insufficient amount of plain(text) evidence: the burden of proof is thus somewhat shifted. In this section, I will analyze the merits and drawbacks of these options, and see to what extent such legislation seems compatible with the privilege against self-incrimination and the presumption of innocence.

8.7.1. Penalize a refusal to cooperate

Penalizing a refusal to cooperate with a lawful order is often used to support the force of such an order. For instance, in Dutch law, if someone called to appear as a witness or interpreter in a court proceeding intentionally fails to comply with the consequent legal duties, he can be punished with up to six months' imprisonment. The same can happen to someone who intentionally refuses to hand over a document which is supposed to be forged. In fact, there

is a general penalization of a refusal to cooperate with a lawful order – for up to three months (art. 184 DCC).

One can therefore well consider using this incitement to enforce a decryption command. However, the threat of three months in prison will not be a serious consideration for Alice, if by obeying the command and uncovering incriminating plaintext, she would risk going to prison for many years. (This was a major gap in the initially proposed extension of the decryption command to suspects in the Computer Crime Act II: it proposed no specific enforcement, and so, if Alice refused to decrypt, she could only get three months in prison.) The punishment for not decrypting and the punishment for the primary offense must somehow be proportionate.

With drunk driving, the legislature has chosen the simplest solution. If you refuse to breathe or give blood, one may safely assume your blood was brimming with alcohol (or why would you refuse to cooperate?), and thus it is acceptable to punish a refusal to cooperate with the maximum punishment that is possible for drunk driving. A difference with a decryption command, however, is that with drunk driving, the primary offense of the suspect is obvious and one-dimensional, and the punishment only depends on the amount of alcohol in one's blood. That makes it reasonable to give someone the maximum punishment in case he refuses to cooperate (this works in effect as a burden-of-proof reversal), and the suspect can exonerate himself by complying. A crypto case, on the other hand, is not one-dimensional. Often, the plaintext is needed to determine just which offense the suspect committed (trafficking soft drugs? or hard ones? or participating in a criminal organization? Forgery? or tax fraud?), and the corresponding maximum punishments may vary considerably. More importantly, a breath or blood test is the only way to prove drunk driving – there are simply no alternatives; this makes it easier for the legislature to punish a refusal to cooperate, as otherwise the offender would easily go unpunished. With decryption commands, however, there may be sufficient other ways to gather evidence (often, there will be other sources of evidence, and, at least theoretically, the police can first try practical attacks on the ciphertext, e.g., guess the password); an encrypted file can never, I imagine, be the single source of evidence of a crime. It is true that in those (few) cases in which the encrypted files are the objects on which the evidence hinges, a refusal to decrypt will block the case. However, unlike with a breath or blood test, to penalize the refusal as such with the maximum punishment for the primary offense seems contrary to the subsidiarity principle. After all, the fact that the breath or blood test is the only way to provide evidence makes it possible to equate a refusal to cooperate with the primary offense; with encrypted files, the refusal to cooperate blocks only part of the investigation, which implies, in my view, that it cannot be equated with the primary offense.

So, in penalizing a decryption refusal, it is not that easy to find a proportionate punishment. Can one set a general maximum of, say, twelve years on a refusal to cooperate with a decryption command? The burden of proof would be all the more heavy on the prosecution as the punishment for non-cooperation is larger: the proportionality principle demands that the relationship between crime and punishment should be proportionate, and to send someone to jail for over ten years for the subsidiary offense of not complying with a legal order is easily disproportionate – unless there be overwhelming evidence that the encrypted file is incriminating, that it is the only missing link for proving a very serious

offense, and that the suspect can decrypt it. In that case, I do not see a reason why the suspect could not be easily convicted for the primary offense (compare 8.7.3: if the evidence is that strong, common sense will lead the judge to gain the conviction that the suspect is guilty).

The problem, then, is finding a middle way between a low punishment (which is little incentive to cooperate, and therefore ineffective) and a high punishment (which lays an almost impossible burden of proof on the prosecution). In Belgium, parliamentarians Bribosia and Maximus have proposed a law to set a punishment of maximum five years on a refusal to cooperate with a decryption command. Their proposal lacks detail (it does not indicate, e.g., whether the command can be given to suspects, although the aim of the proposal indicates it could), but they do explain the (relatively high) punishment:

“The information in the encrypted messages could yield him a conviction. If the person does not want to give the key, the court has no evidence at all against him, and he can go free. By providing for a heavy penal sanction, one wants to incite the citizens to cooperate.” [Bribosia]²⁵

Is five years an acceptable middle way, though? It seems high enough to incite many people to cooperate. Indeed, it virtually creates a Prisoner’s Dilemma situation in which a suspect can choose between the certainty of five years on the one hand, and the risk of either a potential higher sentence or freedom on the other. It seems an interesting game theory question just at how many years the turning point lies between non-cooperation and cooperation for the average Prisoner.²⁶

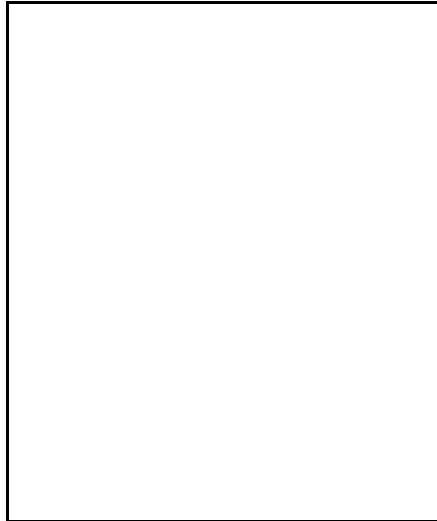
Criminal justice is not game theory, however. A sentence of five years for a simple refusal to decrypt a particular document is high enough to lay a heavy burden of proof on the prosecution. Not only should the prosecutor make a reasonable case for the document being incriminating and a missing link in the evidence of the primary offense,²⁷ but he must also give evidence that it is in the suspect’s power to comply with the order. This is one of the crucial issues at stake in any proposal to command decryption.

There are several arguments that may support a claim that Alice knows her passphrase. For instance, if Alice has (very) recently signed a message (which can be proven with her public-key certificate), it shows that she knew her passphrase recently, at least for her private signature key. If she uses this same key also for confidentiality encryption (which, although

25 Unfortunately, the proposal goes on to say: “With the system of ‘random’ keys, it can of course happen that the person who sent or received it can no longer decipher it (the judge should surround himself with experts who can tell). That does not, however, prevent the person involved from knowing the contents of the message by heart.” I am afraid this indicates Mme. Bribosia and Mme. Maximus have not thought over their proposal well; even if criminals have such good memories, would they be naive enough to tell the police? Or would the MPs have them go to jail for not knowing the messages by heart?

26 An interesting issue is that with a high punishment for the refusal and with sufficient evidence that the ciphertext is a missing link in the evidence, the fact that the suspect refuses to decrypt will almost certainly imply that the ciphertext is indeed seriously incriminating. Consequently, the police could try a brute-force attack on this particular ciphertext – they might buy a Cray supercomputer specifically for these cases, or set up a distributed attack using all police computers’ idle time.

27 I disregard the option of creating a general criminal sanction on a refusal to decrypt for the police regardless of an investigation. It is too close to prohibiting cryptography as such, which I do not consider acceptable (Chapter 6½). Compare 8.7.2.



not advisable, is a common practice with, especially, PGP users), then Polly will have a good case. Another supporting argument is that it seems illogical for Alice to keep encrypted data on her hard disk if she cannot decrypt them anymore. Indeed, a natural prerequisite for using cryptography for stored data in the first place is the future ability to decrypt. Especially with recently encrypted files, one can suppose that Alice will (or should) remember her passphrase.

On the other hand, Alice can use a whole range of retorts against the claim that she knows the passphrase. For instance, she can claim that she is backing-up some encrypted files for Carol, or that she downloaded from a news group some obscure but interesting-looking file which she subsequently forgot. With files having an old

date, she can claim that they were encrypted with some key she has not used for a long time (remark that Alice can anticipate this by setting back the computer clock by five years before storing the encrypted file), and that she simply does not bother cleaning her hard disk every once in a while. Or she might suggest that it is a file in an exotic word-processing format someone once sent her for comment.²⁸ Most of these claims are not particularly probable, but depending on the circumstances, they may be sufficiently convincing (or rather, they may not be sufficiently unconvincing) to argue that indeed, Alice is not able to decrypt. Especially the claim that the file was encrypted a long time ago with a key pair no longer in use can be convincing, I think. For the kind of criminals at issue here, storing incriminating information on a durable diskette or hard disk, there is ample opportunity to anticipate a decryption command with such a retort.

The question whether someone is able to decrypt could to a certain extent be answered by using a legal concept known as *Garantenstellung* ('vouching'). The concept is used in German law to determine liability for an offense of omission. If someone has legally 'vouched' for protecting something specific, or for protecting against a specific threat, he will be liable if he omits preventing damage resulting from the threat. The 'vouching' is determined from the person's (legal) position or from earlier acts. For instance, a close relative living in the same house will be criminally liable for not saving someone from death by starvation, because by his relationship he 'vouches' for protecting the life of his relative. A neighbor does not (legally) vouch for this and cannot therefore be prosecuted for criminally negligent homicide. Another example is the liability of land owners for waste disposal: if a land owner does not remove waste deposited on his land by third parties, he may be

28 Cypherpunks often like to suggest that a suspect can claim that she is just keeping long strings of random data on her hard disk. This argument will not convince any judge – unless perhaps the suspect is a cryptographer or a compulsive mathematician.

prosecuted for endangering the environment through waste disposal; his position as owner of the land implies that he vouches for protecting the land from polluting waste [Schmitz].

The concept of *Garantenstellung* could be transposed to suspects failing to decrypt.²⁹ If by her position or former acts, Alice has ‘vouched’ for ‘protecting’ the encrypted data, she can be held liable for not decrypting: her position or acts imply that she ought to be in the position to decrypt, whether or not she can in reality. In some cases, the prosecution can use this line of reasoning, if it can prove that Alice holds such a position. For instance, if Alice is the information manager or computer expert of a criminal organization, she vouches for her decryption capability by her position. More in general, if circumstances imply that Alice is in a position in which she ought to be able to decrypt, the burden of proof will be on her to argue why she is not able to; if she cannot argue thus, she will be held liable for having incriminating ciphertexts. Such a ‘vouching presumption’ can be used to assign the burden of proof of decryption capability. A *Garantenstellung* may help in a few cases, in particular with well-organized and automated criminal organizations, and with certain computer criminals.

However, if the claim that Alice ought to be in a position to decrypt is to lead to a conviction for refusing to decrypt, the standard of proof should be high. There should be compelling evidence that Alice’s position is such that she has ‘vouched’ for being able to decrypt in the future. Absent such evidence, the judge will have to weigh the arguments of the prosecution and of the defense why Alice is or is not able to decrypt. In many cases, I think, Alice will have to be given the benefit of the doubt if she claims she no longer uses the key pair at issue.

Apart from this proof issue, there is another, more fundamental argument against the approach of convicting people for refusing to decrypt. Penalizing refusals to cooperate with legal orders are *instrumental*: they are not reprehensible in themselves, but they serve to ease investigation. If Alice is a criminal, we want her to be punished for her crimes. Penalizing a refusal to decrypt is an alternative way to punish Alice – if we cannot get her at the front, we catch her at the backdoor. It may have the same effect when it comes to keeping Alice out of society for a while, but it gives less satisfaction to our sense of justice: her crimes go unpunished (or she was even innocent in the first place). Instrumental penalization may be practical in some cases (such as drunk-driving tests), but it inflates the moral justification of criminal justice. In this case, the (potential) effect of penalizing a refusal to decrypt seems simply too small to justify such inflation.

8.7.2. Penalize cryptocriminal use

A similar way to incite a suspect to obey a decryption command, is to penalize crypto use if this hampers investigation. The issues at stake here are largely similar to penalizing a refusal to decrypt, but the proof issue may be significantly easier for the police. Consider Mr. Salabiaku, who was convicted for drugs *smuggling* merely because he *carried* them. He might have acquitted himself if he had explained how he came to carry the drugs, but he did

29 This, of course, is very different from the German application of the concept; by transposition I mean that one might apply the line of reasoning rather than the legal circumstances.

not. In fact, he had been warned by a customs official not to take the suitcase he came to collect, for there was reason to suspect it contained drugs. Still, Salabiaku had taken the suitcase and, without opening it, had walked through customs. After his arrest, he was prosecuted for smuggling drugs, as the French customs law said that possession of drugs in such a case means smuggling. Only if the defendant establishes a case of ‘force majeure beyond his control’ can the defendant exculpate himself. The European Court argued that the presumption of guilt in this law was not irrebuttable, as there were enough safeguards built-in through case law to allow someone to argue force majeure (and people had been given the benefit of the doubt by the courts). The French court had shown “scrupulous respect for the presumption of innocence”, as it had acquitted Salabiaku of the *criminal* offense of importing narcotics, giving him the benefit of the doubt, and only convicting him for the *customs* offense of smuggling. In the latter, it had not automatically resorted to the presumption of guilt laid down in the law, but had inferred from the fact that Salabiaku had not heeded the customs official’s warning that there were no arguments to rebut the evidence.

The Salabiaku case shows that it may be possible, under certain conditions, to “penalize a simple or objective fact as such, irrespective of whether it results from criminal intent or from negligence”. The main conditions are that in the application of the law, there must be sufficient safeguards to maintain the rights of the defense, notably a practical chance for the defendant to argue against the presumption of guilt, a chance which the courts must explicitly give him. A caveat is that in Salabiaku, a customs law was involved, with according subject matter (it is difficult for customs officials to prove smuggling, but easy to prove possession).

Still, the case suggests an interesting analogy to the crypto question. Can a state penalize the possession of a ciphertext as such, with an acceptable defense if the suspect decrypts? There have been several proposals to this effect, notably from US senators and representatives. Three bills discussed in 1997 contained provision to this effect. The Security And Freedom through Encryption (SAFE) Act of Rep. Goodlatte, e.g., would criminalize crypto use with the intention to cover up a federal felony; Senator Leahy’s bill, the Encrypted Communications Privacy Act, would penalize the use of encryption in furtherance to a felony, if the encryption is intended to obstruct investigation; and senators’ Kerrey, McCain, and Hollings Secure Public Network Act contained a similar provision. The Ashcroft and Leahy E-PRIVACY Act of 1998 would also criminalize the use of encryption to conceal ‘incriminating’ communications or information during the commission of a crime. All these proposals are ultimately intended to ease proof issues: if Alice threatens to get away with insufficient evidence for a criminal offense because she has used cryptography, you catch her instead for the crypto use. It seems to me that this does not solve the proof issue, because, if there is not enough evidence to prove a criminal offense, how can you prove crypto use ‘to cover up the felony’? You either lower the requirement of proof for the offense (which is the burden-of-proof reversal of section 8.7.3), or you penalize crypto use irrespective of a presumed crime.

The latter is an option, but it is not an attractive one. It means that, in principle, everyone who uses cryptography is potentially acting criminally, which he can only undo if he cooperates with a decryption command. That is dangerously close to criminalizing cryptography as such, which, as I argued in Chapter 6½, is absurd. Moreover, if the penalization is intended to encourage suspects to cooperate with a decryption command, the

same problem of the punishment as in section 8.7.1 holds: if it is too low, no criminal will cooperate, whereas a high punishment is disproportionate – and the middle way seems the worst rather than the best of both worlds.

One would have to resort, then, to a more restricted offense, say, criminalizing crypto use only if this obstructs the investigation of a crime, regardless of the intention. This is a straightforward provision, which does away with the issues of proving the ciphertext is incriminating and a missing link in the evidence of the primary case.³⁰ Decrypting on command (or having used key escrow) can be an affirmative defense, to make rebuttable the presumption of guilt inherent to the provision. There remains, however, the familiar problem of the maximum punishment: three months? The maximum of the (presumed) offense under investigation? The arithmetical mean of these?

Again, my main objection to such a provision is that it is instrumental, creating an offense of something which is in no way reprehensible in itself. If it really helped in easing investigation, one can be willing to accept this. I am skeptical, however, as to the efficacy of such a provision. If it is applied carelessly by the courts, the prisons will fill up with innocent crypto users who forgot their keys. The risks of catching the wrong ‘criminals’ can only be strictly limited if the provision is applied by the courts with scrupulous respect for the rights of the defense. In that case, however, if the courts are sufficiently lenient in accepting a defense for a refusal to decrypt (e.g., if Alice argues she no longer uses the key, or that decrypting would infringe her privacy, and if she can make this plausible), it will not often lead to a conviction. The same remarks about the *Garantenstellung* (see 8.7.1) apply here: it will only be in a few cases of well-organized and computer crime that the prosecution can argue that Alice is in a position in which she ought to be able to decrypt.

There is yet another, similar option: use a refusal to decrypt to raise the punishment for the primary offense. Sentencing guidelines or an aggravating circumstance in a penal provision may provide that if there are encrypted data the suspect refuses to decrypt, the punishment to the offense is to be increased with a certain percentage of the maximum punishment. This does nothing, however, to solve the law-enforcement problem, since in this case, there should be sufficient evidence in the primary case anyway to convict the defendant, regardless of the encrypted data. Therefore, I do not consider it an option.³¹

30 There remains the issue of proving it is ciphertext rather than random noise, something which expert witnesses for the prosecution and for the defense have to fight out, and which seems doable. See 8.7.3.

31 Also remark that it is already the case that the course of action adopted by the defendant during the proceedings is a factor in determining the punishment. A cooperative defendant may be given a somewhat lower sentence than an obstinately obstructive defendant. Remaining silent to all questions, although it is a fundamental right of the defendant, may thus be weighed by the judge if it amounts to a ‘negative attitude’: once a judge has concluded guilt, no legal rule prevents the judge from taking into account a ‘negative attitude’ in determining the punishment. [HR 18 December 1984]

8.7.3. Reverse the burden of proof

*Their silence was by politicians used,
Their teeth opened with phrase, their puppet heads
voided comic balloons: their speaking death
Supposed his debt, and gave him much advice.
(Howard Nemerov, Who did not die in vain)*

Rather than punish someone for refusing to decrypt or for criminal crypto use, one can also use the refusal or the ciphertext as evidence that Alice has something to hide – and thus convict her of the primary offense. Here, the privilege against self-incrimination meets the presumption of innocence: no-one can be supposed guilty until proven so in a legal procedure – something which the prosecution must prove (art. 6 para. 2 ECPHR). One cannot reverse the burden of proof for the suspect to prove her innocence. On the other hand, there is no absolute prohibition of a shift in the burden of proof, as *Salabiaku* attests, and silence can sometimes be used as evidence. This section investigates the use of ‘cryptographic silence’ as evidence in the primary offense.

If Polly asks Alice to decrypt, and Alice refuses, can the judge use this as evidence that Alice is hiding something incriminating, and consequently, infer that Alice has done it? There is some case law on the use of silence as evidence, and I shall accordingly treat a refusal to decrypt as remaining silent on a certain question. The right to remain silent is not absolute, in the sense that silence would never be usable against the suspect. Such, at least, is the view of the European Court, which in *Murray* – in a rare pun – notices that “established international standards in this area, while providing for the right to silence and the privilege against self-incrimination, are silent on this point.” From this silence in international standards, they infer, “if the evidence against the accused ‘calls’ for an explanation which the accused ought to be in a position to give that a failure to give any explanation ‘may as a matter of commonsense allow the drawing of an inference that there is no explanation and that the accused is guilty’.” Murray was asked to explain his presence in the house where an IRA hostage had been held, and his silence on this point – after several warnings that his silence could and would be used as evidence against him (in accordance with an exceptional Northern Ireland law) – was taken by the courts as evidence that he could not acquit himself. The European Court allowed this, “having particular regard to the situations where inferences may be drawn, the weight attached to them by the national courts in their assessment of the evidence and the degree of compulsion inherent in the situation.” Moreover, the Court considered the following circumstances:

- there were appropriate warnings as to the legal effects of remaining silent,
- there was a prima facie case against the accused,
- the evidence ‘called’ for an explanation,
- the trial judge had a discretion whether an inference should be drawn from the silence,
- the judge had to explain the reasons for the decision to draw inferences, and this decision was subject to appellate review.

Local precedents for reversing the burden of proof

Although the Dutch Supreme Court does not allow using silence as evidence, there are precedents for laws that reverse the burden of proof. In several General Municipal Ordinances (GMO), carrying subversive stuff is taken as an indication of guilt until proven otherwise. For instance, in Wassenaar, it is forbidden to carry false keys, rope ladders, lanterns, or any burglary tools on the road at night; the prohibiting does not apply when it is made plausible that the carrying of the tools does not happen with the aim of burgling (art. 134a GMO Wassenaar, see HR 7 June 1977). Likewise, Groningen proscribes carrying glue, paint, tar, chalk, or any other coloring or dyeing substance in public at night, unless the carrier makes a reasonable case that these goods are not meant for illegal sticking or graffiti (art. 17 GMO Groningen, see HR 13 December 1977).

Contrary to the European Court, the Dutch Supreme Court does not incline to allow using silence as evidence. In a recent case, the DSC adhered to the principle that a refusal to testify cannot in itself be used as evidence [HR 19 March 1996, *NJ* 1996, 540]. The Court, however, did go on to say that such a refusal may have consequences in court, for instance, when the defendant puts forward a ‘Meer & Vaart’ defense, i.e., a defense that gives an explanation which is compatible with the evidence but which contradicts the alleged offense. In this case, the defendant had, out of her own accord, provided an alibi for the time of the murder. When the alibi proved false, she refused to explain why she had construed the alibi without being asked. The Court of Appeals inferred from this construing of a false alibi that she must have known when the murder had been committed, and, consequently, that she had done it. The Supreme Court did not allow the use of this inference, as the Court of Appeals had used the defendant’s silence as evidence that the alibi was false and intended to cover up the truth, and as it had used this falseness as evidence that she had committed the murder. However, the Supreme Court would have allowed, it implied, using silence to reject a defense which would, for instance, have explained her presence on the spot at the time of the murder without her having committed the murder (e.g., because she had an appointment with the neighbor). If such a defense is put forward, the court must explicitly explain why it rejects this explanation – and a refusal of the defendant to answer questions related to this defense *can* be used by the court to argue that the defense does not hold.

The difference between *Murray* and the Dutch silence case, then, is the *use* of the silence: the European Court allows its use under specific conditions as direct evidence of the offense, whereas the Dutch Supreme Court only allows it to refute a specific defense from the defendant.³² But is this difference so fundamental as it looks at first sight? If one considers the verdicts carefully, it may turn out that there is a difference in approach rather than in essence.

The *Murray* case was a specific one, dealing with a peculiar Northern Ireland law that allows drawing inferences from silence in specific circumstances. The European Court did

32 A more recent case seems to go further than this in allowing silence as a basis for the proof. The failure of a defendant to explain how he came to possess a bus card stamped at the place and time of the offense was considered a reason on which to base the proof that it was the suspect who had committed the offense, since the bus card supported the claim of witnesses that they recognized this particular suspect. Not explaining something which supports a basis for the proof, can thus apparently be used to confirm evidence that establishes guilt. [HR 3 June 1997]

not review the law, but only its application to Murray. The main question was whether there was enough evidence to establish a ‘prima facie case’,

“i.e. a case consisting of direct evidence which, if believed and combined with legitimate inferences based upon it, could lead a properly directed jury to be satisfied beyond reasonable doubt that each of the essential elements of the offence is proved”.

And in each particular case, “the question is whether the evidence adduced by the prosecution is sufficiently strong to require an answer.” In his dissenting opinion, Judge Walsh argued for more evidence to make a prima facie case:

“In a criminal prosecution the burden of proof of guilt beyond reasonable doubt always rests on the prosecution. Therefore a prima facie case means one in which the evidential material presented by the prosecution, if believed and not rebutted, is sufficient in law to establish the guilt of the accused.”

This seems more in line with the reasoning of the Dutch Supreme Court, which prohibits using silence to contribute to establishing guilt.

So, just what is a ‘prima facie’ case? In the view of the European Court, it is a case with a lot of evidence, perhaps not entirely sufficient to prove guilt of itself, but which, if supplemented with common-sense inferences based upon it, would be sufficient to prove guilt. In the view of the Dutch Supreme Court, like in Walsh’ view, a prima facie case is directly sufficient to prove guilt. Does that mean that the Dutch Supreme Court rules out common-sense inferences? No – a Dutch judge can use his observation and common sense to gain an inner conviction of the defendant’s guilt. The difference is that he does not (have to) say so: he merely lists the evidence, and concludes guilt; in the Murray case, the court explicitly mentioned its ‘common-sense’ inference. It may really be a matter of open versus hidden, or explicit versus implicit, use of evidence, hence the stress of the European Court on the fact that in Northern Ireland, “where trial judges sit without a jury, the judge must explain the reasons for the decision to draw inferences and the weight attached to them. The exercise of discretion in this regard is subject to review by the appellate courts.”

I think the main difference between the European Court and the Dutch Supreme Court’s views is not so much the amount of evidence needed to establish a ‘prima facie’ case, but rather the way the evidence is presented. A prima facie case is a case in which there is virtually enough evidence to conclude guilt. There may be just a hairline missing for an obvious conclusion of guilt – and common sense is used to bridge this hairline’s gap, be it explicitly or implicitly.

If this assessment is correct, then both the European Court and the Dutch Supreme Court would allow the use of silence as evidence, since common sense tells us that something is rotten if someone remains silent when circumstances cry out for an explanation. The conditions for using silence, however, are severe. The other evidence must be enough to base a common-sense conclusion of guilt upon, the defendant must not have been (unduly) pressured to testify,³³ and the evidence must ‘call’ – or, I would say, ‘shout’ – for an explanation the defendant is unwilling to give.

33 In *Murray*, the European Court concluded that Murray had not been unduly pressured *because of* the fact that he had been able to remain silent, an *ex post* inference that would hardly meet a logician’s approval.

There remains, then, little room for using silence, but still, it is some room. There are three stages of judging whether evidence is sufficient – evidence must conform to the minimum legal rules,³⁴ it must have been obtained legitimately, and it must convince the judge that the suspect did it. Cryptographic silence can be used in the last stage: to strengthen the judge's conviction. It can not be used in the first stage of making evidence conform to the minimum legal rules, as these are already sufficiently weak: one witness testimony together with some independent evidence which supports part of the charge will suffice. Using silence to supplement the minimum legal rules would constitute a radical change in Dutch criminal procedure law. Moreover, in the problem at issue, the evidence will almost always be legally sufficient to meet the minimum rules; the key issue is whether the evidence convinces the judge.

So, the refusal to decrypt or deliver the key might be used as (supporting) evidence that Alice did it, but only if:

1. there is enough other evidence against Alice that, combined with her refusal, allows a common-sense conclusion of guilt,³⁵
2. Alice has not been pressured by Polly to give the key (echoing the European Court, if she does not give it, she has apparently not been unduly pressured),
3. the ciphertext at stake must 'call' for an explanation, and
4. there is enough evidence that Alice is able to decrypt.

I shall refer to these as the 'Murray conditions'.

The fourth condition (that Alice 'ought to be in a position to decrypt') requires considerable supporting evidence, and may lead to complex arguments in court (compare 8.7.1); it may, however, require less argument than in penalizing a decryption refusal, since 'ought to be in a position' is more objective and general than a 'foregone conclusion' that Alice knows the key. Can one say that, in general, someone using cryptography 'ought' to remember the key, and thus lay the burden of proof with Alice to argue that she did forget it? Yes, one can, but Alice will have several ways to argue that in this particular case, she – alas – does not know the passphrase (see 8.7.1). Here, the *Garantenstellung* (see 8.7.1) seems the best device to assign the burden of proof whether Alice is able to decrypt. If the prosecution shows that Alice is in a position in which she has 'vouched' for a decryption ability (notably, because she is the information manager of a criminal organization, or because she is a very experienced in encrypting crucial information), then the burden of proof is on Alice to argue why she cannot decrypt. Note that it will not be often the case that Alice 'vouches' by her position or her person for a decryption ability.

The third condition will likewise not always be easy to meet. Does the fact that Alice has encrypted her stored files and her e-mail messages 'call' for an explanation? If Alice has encrypted her hard disk or diskettes, she may assert she is just cautious with information security, having read stories in the newspapers of burglars stealing compromising diskettes

34 Dutch criminal procedure law has a few minimum rules to which evidence must conform: a conviction cannot be based solely on the basis of one witness, nor on the sole basis of a confession, nor on the basis of only anonymous statements.

35 Note that this is stronger than Andersen and Landrock's condition of circumstantial evidence (see sidebar in 8.6).

even from public prosecutors. In the case of a few encrypted files on an otherwise plaintext diskette or hard disk, Alice may be called upon to explain their presence. "I just don't want my daughter to see these dirty pictures" may not be the smartest answer, as in that case, the police could request (not command) her to decrypt to acquit herself – if Alice refuses that, the court can refute her 'Meer & Vaart' explanation of the encrypted files. She may resort to explaining the ciphertext as her innermost private diary, in which case Polly must have strong reasons to ask her to decrypt (private letters are not to be delivered, unless there is evidence that they are related to the crime); and here, Alice will have a somewhat stronger (though still not very convincing) case arguing her refusal (her privacy is her inner sanctum). If Alice is smart, she will use a disk encryptor to bypass the necessity of having to explain why some files are encrypted where others are not.

There is also the point of proving something *is* in fact a ciphertext, rather than random garbage. With recorded communications, Polly will be hard put to argue that it is a ciphertext: if she missed out one or two bits, or if she did not start the recording at the exact beginning of the conversation (and this is not easy with recording bits), the result will be garbage and not a ciphertext. How is she to argue that the recording is a ciphertext? With e-mail messages, it may be more viable to argue it is a ciphertext, especially if a header announces an encrypted message. The same holds for stored data. In these cases, it is logical to ask the sender or holder what the random data are doing there – you normally do not keep random garbage on your hard disk, let alone send it to someone. There may be possible explanations (e.g., using a random stream to generate crypto keys, or to research properties of random data), but at least the presence of random bits in an e-mail message and on a data carrier 'call' for an explanation, and generally Polly will be able to make a good case that these random data are, in fact, ciphertexts.

Then, as many have suggested, there is the chance that smart criminals will use steganographic means to 'hide' encrypted files on their computers. Alice may hide a ciphertext in images or sound files, and then Polly has a hard task in arguing that the files contain hidden data (she can, see Chapter 4, but it requires a lot of investigation, and a convincing expert witness). And if Alice stores some fifty encrypted dirty pictures on her hard disk, which she – reluctantly, being a good actor – decrypts on Polly's command, there is a good chance Polly will disregard the fifty-first ciphertext; or she may fail to investigate whether the decrypted dirty pictures contain hidden data. Alice may even encrypt some "mildly incriminating dummy messages" to decrypt before Polly's eyes, in order to hide the really incriminating texts (as Schneier claims, a pair of Israeli spies once did this [Schneier, 228]). Although Polly can always find out in principle, I think the options for Alice are broad, and if Alice is determined, she will fool Polly. This is not to say that Polly will always fail – not all criminals are that smart or prepared. There may be sufficient cases in which the presence of encrypted files on a computer calls for an explanation the suspect is unwilling to give. And in that case, this refusal may be used in court as supporting evidence, provided the other conditions are met.

The question that remains is whether Polly will be satisfied with this option. If the use of cryptography as such (with e-mail or a hard disk encryptor) is not sufficiently uncommon to call for an explanation, which I think will often be the case, it is only the presence of a few encrypted files on a computer or diskette that may call upon a suspect to explain why they

are there. For criminals who are aware of this problem, there are options to blur the existence of incriminating ciphertexts. It is the less prepared and less wary criminals that may be caught with inexplicable ciphertexts – this may well be the largest part of the criminal society, if you consider how many criminals have incriminating conversations over the telephone. Still, the other conditions for using the ciphertext as supporting evidence hold: there must be a prima facie case against Alice, and there must be considerable evidence that Alice ought to be able to decrypt (which may be difficult if Alice has not ‘vouched’ for her decryption ability).

And this brings me to the ultimate question here. If there is enough evidence to make a prima facie case, which means that using common sense is enough to base guilt upon this evidence, then what is the extra evidential value of a refusal to decrypt? It may add to a judge’s conviction of guilt, but it can hardly co-establish it. With current law and case law, a refusal to decrypt may bridge the (hairline’s) gap between strong evidence and sufficient evidence, but the *Murray* conditions for using this explicitly are so heavy that this will only work in few cases in practice.

To alter this, and be more lenient in using silence as supporting evidence than current case law allows, does not seem acceptable to me. The above use of silence as evidence has explicitly explored the margins of the right to remain silent, and if one crosses that border, the presumption of innocence is violated. In my view, *Murray* leaves the presumption of innocence intact:³⁶ it is like adding a weight to a pair of scales so that the scales only just remain in the same fixed position (namely, where the defendant is presumed innocent). If one adds just a milligram more, the scales start to move, and a portion of the burden of proof is referred to the defendant. One could decide to allow that for criminal-political reasons, but in my opinion, the presumption of innocence is at the core of criminal justice, and it can not be scaled down without undermining the credibility of the rule of law. One can also, of course, expect the European Court to turn down a significant burden-of-proof shift as a violation of the presumption of innocence.

8.8. Assessing the decryption command

8.8.1. The decryption command in current law

A decryption command can be given to network and service providers, to non-suspects, and to people working in corporations (except when they conduct the business as a sole proprietorship (US) or when they are liable as executives for corporate offenses (Europe), and if the act of production is testimonial). Self-escrow agents within corporations (and, of course, external escrow agents) will be useful to obtain keys or plaintext; the current punishment for not complying with a decryption command can be considered adequate for inciting them to cooperate, as they have little reason not to. The option of demanding non-suspects to decrypt can also be useful in organized crime cases, or in other cases involving

36 “Nor can it be said, against this background, that the drawing of reasonable inferences from the applicant’s behaviour had the effect of shifting the burden of proof from the prosecution to the defence so as to infringe the principle of the presumption of innocence.” [*Murray*, at 54]

various suspects, as Bob can be required this way to provide evidence against Alice. Here, however, the punishment for not complying may be too low to incite accomplices to cooperate.

When it comes to asking suspect Alice to decrypt, the privilege against self-incrimination starts to assert itself. Polly can command her to deliver a stored key or a smart card with the key, if she knows Alice possesses it, but generally, this will be passphrase-protected. The key issue is whether Polly can ask Alice for the passphrase (or for the key, if she knows this by heart). Case law of both the European Court and the US Supreme Court suggests that such a command can be compatible with the privilege against self-incrimination, provided that the police can argue that Alice is able to decrypt, to the extent that Alice's ability is a foregone conclusion (in *Funke* terms: the police must be sure of the fact that Alice can decrypt). This will be possible in few cases.

Currently, therefore, there is not much room for Polly to demand decryption. When one investigates the options for the legislature to create a specific power for the police to demand decryption, the rationale of the privilege against self-incrimination suggests that, in principle, such a power can be compatible with the privilege: it provides reliable evidence (the passphrase or key either works or it does not). However, the same *Funke* requirement should hold, namely, that there is compelling evidence that Alice is able to decrypt. Case law, then, has already explored the borders of the privilege against self-incrimination; the legislature can only make this explicit, but can hardly extend beyond this in light of current law. For the purpose of this book, I shall assume that a decryption command can be given to suspects under these strict conditions. The real issue at stake is how the legislature plans to enforce this command: these are the options to consider.

8.8.2. Options for enforcing a decryption command

Together with a power to demand decryption, the legislature should create an enforcement of this power, as otherwise Alice will kindly refuse to cooperate. There are three major options for inciting suspects to cooperate.

Option 8.1 Penalize a refusal to decrypt

The legislature penalizes a refusal to obey a lawful command, given in the investigation of a serious crime, to decrypt stored encrypted data and encrypted one-way communications. This is a special clause overruling the general criminal provision of refusing to cooperate with a legal command. The legislature must determine the maximum punishment for the refusal after careful consideration of the trade-off between effectiveness and the rule of law; it should be high enough to incite (serious) criminals to decrypt, yet be low enough not to create an insurmountable burden of proof for the prosecution to show that the data are incriminating and that the suspect is able to decrypt; nor should it be a disproportionate punishment for forgetting a crypto passphrase. It can be a fixed maximum, or it can be related to the maximum punishment for the primary offense.

The legislature may at the same time consider extending the power to demand decryption to be given under less strict circumstances (than the *Funke* requirements), i.e., with less than aggravating evidence in the primary offense, or with less than strong evidence that the encrypted data are incriminating for the primary offense.

The legislature can consider extending the provision to cover encrypted two-way communications, if it turns out that technology allows users in principle to decrypt after the communication has ended.

Option 8.2 Penalize crypto use if this obstructs investigation

The legislature penalizes having stored data in encrypted form if this obstructs a specific investigation of a serious crime. The suspect can exonerate himself by decrypting. The legislature must determine the maximum punishment for the encountered crypto after careful consideration of the trade-off between effectiveness and the rule of law; it should be high enough to incite (serious) criminals to decrypt, yet be low enough not to create an insurmountable burden of proof for the prosecution to show that the data are incriminating and that the suspect is able to decrypt; nor should it be a disproportionate punishment for forgetting a crypto passphrase. It can be a fixed maximum, or it can be related to the maximum punishment for the primary offense.

The legislature can consider extending the penalization to cover sending or receiving encrypted e-mail. Likewise, the legislature can consider extending the provision to cover encrypted two-way communications, if it turns out that technology allows users in principle to decrypt after the communication has ended.

Option 8.3 Shift the burden of proof

The legislature enacts a law stipulating that the refusal to decrypt stored encrypted data or encrypted e-mail encountered during the investigation of a serious crime can be used as incriminating evidence in the case. The conditions for the judge to use a decryption refusal as evidence are the Murray conditions:

1. there is enough other evidence against the suspect that, combined with her refusal, allows a common-sense conclusion of guilt,
2. the suspect has not been pressured by the police to give the key;
3. the ciphertext at stake must 'call' for an explanation, and
4. there is enough evidence that the suspect is able to decrypt.

The legislature can consider weakening these conditions, notably the fourth and, to a less extent, the first and third, after a careful consideration of the trade-off between effectiveness and the presumption of innocence.

The legislature can consider extending the provision to cover encrypted two-way communications, if it turns out that technology allows users in principle to decrypt after the communication has ended.

8.8.3. Applying the criteria

How do these options relate to the principles for striking the crypto balance?

1a. Privacy and the right to confidential communications

The options do not as such infringe the right to privacy: everyone can use as much crypto as they want. It is only when Alice becomes a target for investigation and when there is considerable evidence against her, that she may have to decrypt and reveal privacy-sensitive information. For a law-abiding Alice, this will occur rarely, and if it happens, she

may not be too particular about her privacy if she can thus exonerate herself. (I assume there are good safeguards for Polly to deal with the decrypted information.) The very rare case that law-abiding citizens would be required to decrypt privacy-sensitive information they would not want the police to see, is of too little weight to take into account. (Besides, in such a case, Polly could also allow Alice to have a notary decrypt the information and notify Polly whether it is what she is looking for or not.) In general, then, the right to privacy is not infringed.

The right to privacy might be infringed, however, when the stipulations for the decryption command and the penalty for refusing to decrypt are significantly weakened. That is, if the command can be given when there is less than strong evidence in the first place, or when the decryption command can be given for less serious crimes, the chances for (law-abiding) Alice to have to decrypt privacy-sensitive information will be higher. If the likelihood of law-abiding citizens eventually facing a decryption command becomes such that one can speak of a strict liability when they use cryptography, then (and only then) privacy is at stake. It might lead to people reconsidering the use of cryptography (“What if the police barge in and ask me to decrypt, what if I forget my key?”), which could lead to an infringement of their privacy. Note that the hypothetical case of the police asking law-abiding citizens to decrypt is unlikely, even with weakened conditions for allowing a decryption command; it is more likely to occur in business surroundings, but there, people have considerably less expectation of privacy. Even strict liability for crypto use would not quickly lead to an infringement of privacy.

Comparing the three options, the first two may be considered somewhat more privacy-threatening in the graver versions: if there are comparatively weak conditions for allowing a decryption command and for convicting someone for not decrypting, the question of strict liability will come up more easily. With reversing the burden of proof, strict liability is less privacy-threatening, since there must always be sufficient evidence in the primary case (in other words, weak conditions can only apply to claiming ability to decrypt, not to circumstantial evidence in the primary case); law-abiding citizens would not consider such a measure a reason to use less cryptography.

1b. The right to a fair trial

Where the privilege against self-incrimination and the presumption of innocence are at stake, the right to a fair trial may be infringed, even severely. As long as the decryption command and the sanction for not complying with it remain within the limits set by case-law (*Funke*, *Saunders*, and *Murray* in Europe, *Doe II* and *Schmerber* in the US), the right to a fair trial will be safeguarded. In that case, however, the decryption command will hardly be effective: it will only be applicable in very few cryptocriminal cases, and smarter criminals have good opportunities of anticipating a decryption command with convincing retorts.

If the decryption command is to be more effective, by raising the penalty on not complying, the right to a fair trial may be infringed. Since current case law has, as I have argued, already explored the limits of the privilege against self-incrimination and the presumption of innocence, it is likely that all three options do infringe the right to a fair trial to some extent. It will depend on the modalities of the option whether the infringement

is small or rather severe. For instance, if a low punishment is set for refusing to decrypt or having crypto that blocks an investigation, or if the Murray conditions are adhered to, the infringement will be small (i.e., one could expect the European Court of Human Rights to condone the law if it is sufficiently shown by the government to be necessary in a democratic society). On the other hand, if a relatively high punishment is chosen (for instance, five years) to incite criminals to decrypt, or if the Murray conditions are weakened to shift the burden of proof, the infringement will be significant. Obviously, there is a trade-off between effectiveness and the right to a fair trial.

Of the three options, the burden-of-proof reversal is the most threatening to the right to a fair trial. The presumption of innocence is a more fundamental right for the defendant than the privilege against self-incrimination; the latter safeguards finding the truth rather than the rights of the defendant as such. Depending on the conditions under which a refusal to decrypt can be counted as evidence in the primary case, the infringement of the right to a fair trial range from significant to severe.

1c. The rule of law

As noted, there is a key trade-off between effectiveness and the right to a fair trial (and, less so, between effectiveness and privacy). As such, the rule of law is affected in two ways. If a strong enforcement of a decryption command is chosen, this means more effectiveness and thus, better prosecution of crimes, which is an important benefit for the rule of law, but at the same time, it means an infringement of one of the most important rights safeguarding the rule of law itself. If a weaker enforcement is chosen, compatible with current case law, the effects are reversed. Of course, this is a trade-off that pervades criminal justice: the legislature always has to balance the rights of the defendant with the need to prosecute crimes and convict criminals.

One of the difficulties in the present case is that the legislation would be targeted at serious criminals, who are mostly premeditating, calculating people apt to anticipate police activities. Notably when they store incriminating evidence, one can expect them to be more careful of possible police monitoring than when talking over the phone. If a criminal uses cryptography to hide incriminating evidence, he is likely to be aware of the possibility that the police may one day ask him to decrypt; thus, he can anticipate this by, for instance, using many different key pairs or setting back the clock of his computer (or, perhaps, using a duress escape). This could mean that a decryption command would work least of all with the most serious criminals the legislation would precisely aim at; it may turn out to work in practice only with minor, less serious criminals. Of the three options, reversing the burden of proof under weaker Murray conditions would be best targeted at catching the most serious and calculating criminals (especially if one takes into account a *Garantenstellung*). It is also better compatible with the rule of law in that the criminals are convicted for the primary offense they are charged with, not for instrumental 'crimes'. In any case, the decryption command will not work in many cases in practice, since it would only be allowed as a last resort to finalize the evidence; one can assume that in many cases, the encrypted data will only be part of the overall evidence, and there will not be sufficient evidence that these particular encrypted data are incriminating and necessary for the final evidence. Thus, the

expected effectiveness of the options is, at best, not great (unless one chooses a really severe enforcement that does away with the rights of the defendant altogether).

Another aspect is the potential 'stepping stone' effect of this legislation. Infringements of the privilege against self-incrimination and burden-of-proof reversals are rare in the Dutch law system (as in most law systems). Penalizing a decryption refusal or obstructive crypto use will set another precedent for instrumental penalization and allowing an infringement of the privilege against self-incrimination. Using a decryption refusal as evidence, even under Murray conditions, would be a unique step in Dutch criminal procedure: so far, silence or refusals to cooperate have never been (explicitly) allowed to be used as evidence in criminal cases. It could be a first step on a slippery slope that can ultimately lead to a downfall of the presumption of innocence altogether.

1d. The right to economic development

The right to economic development is not at stake. Indeed, the market would welcome these options as leaving crypto manufacture, sale, and use unharmed, thus reinforcing information security and electronic commerce.

2a. A solution must be workable

The options can fairly easily be implemented: guidelines for the police and courts under which conditions they can give a decryption command and how they should deal with delivered crypto keys and decrypted evidence would suffice. The only difficulty for the legislature in implementing the two first options is to find an acceptable and effective punishment for not decrypting. As I argued above (8.7.1), it will be hard to choose a punishment that is high enough to incite serious criminals to cooperate, yet low enough not to create insurmountable proof issues for the police. These proof issues may be the only problem for the police in enforcing the options in practice. Especially with the third option, the Murray conditions require them to find sufficient arguments that the encrypted data are incriminating and, often more difficult, that the suspect is able to decrypt.

2b. A solution must be internationally compatible

The international component is one of the advantages of these options. Obviously, the options can be implemented in national legislation, regardless of what other countries are doing. Note that the option mainly targets stored information, which will, by definition, be encountered by the national investigation agents (they have (currently) no authority to search abroad). With encrypted e-mail, it is usually only the recipient who is able to decrypt, and he may live abroad. In that case, the police can ask for international legal assistance if the recipient's country has a similar power to command decryption.

2c. A solution must be technologically sustainable

Demanding decryption is independent of the crypto technology used, and so, the options are eminently sustainable.³⁷

³⁷ Well – Ron Rivest recently introduced 'chaffing and winnowing'. [Rivest] This is a procedure in which Alice and Bob exchange authenticated messages interspersed with 'chaff'. That is, the message is not encrypted with a key, but intermixed with random, unauthenticated data. Alice and Bob use a common and secret

Table 8.1 gives a simplified illustration of how the options match the principles.

<i>principles</i>	<i>options</i>	penalize decryption refusal	penalize criminal crypto use	reverse burden of proof
1a privacy		±/+	±/+	+
1b fair trial		±/-	±/-	-
1c rule of law -effectiveness		+/ \pm	+/ \pm	+/ \pm
-general		-	-	-
1d economic development		+	+	+
2a workable		+/ \pm	+/ \pm	+/ \pm
2b international		+	+	+
2c technology- neutral		+	+	+
<i>overall estimate</i>		±/-	-	±

Table 8.1. Demand-decryption options and principles

- *infringes principle*
- ± *has mixed effects on principle, infringes to a smaller extent*
- + *does not infringe principle*

8.8.4. Conclusion

If one is to choose some kind of infringement of the privilege against self-incrimination or the presumption of innocence (the crypto problem, after all, is a serious one), I would choose the option of ‘shifting’ the burden of proof. Penalizing a decryption refusal (let alone penalizing ‘criminal’ crypto use) is an instrumental law which creates complex proof debates, and one which resorts to catching criminals the wrong way. If cryptography hampers an investigation, we want the offense at issue, not the hampering of the investigation, to be punished. ‘Shifting’ the burden of proof is in some way compatible with the presumption of innocence, but only if several – severe – conditions are met. Most notably, there must be strong evidence against Alice (more or less a prima facie case), her refusal to decrypt must call for an explanation, and there must be evidence that Alice is able to decrypt. Moreover, she may not be unduly pressured into cooperating, e.g., through threat of violence (humanity is a lower limit here).

authentication key with which they can distinguish the ‘wheat’ (the true plaintext) from the ‘chaff’. Since authentication keys should be exempt from delivery to the police (or otherwise the police could easily forge evidence), Polly cannot demand Alice or Bob to deliver the authentication key. She can ask them to ‘winnow’ the ciphertext, but she has no way of knowing whether Alice or Bob provides her with ‘wheat’ or ‘chaff’. The scheme thus resembles a duress code.

In choosing an enforcement variant, two major trade-offs have to be made. The first is *effectiveness versus proportionality*. In penalizing a refusal to decrypt or 'criminal' crypto use, the punishment for the refusal must meet the middle between a low punishment that is ineffective (it will not incite serious criminals to cooperate), and a high punishment which, if it is not to be disproportionate, is ineffective as well (it creates an insurmountable burden of proof for the prosecution). A similar trade-off has to be made by the court if the refusal is to be used as evidence in the primary case: the lower the burden of proof on the prosecution to show that Alice is hiding incriminating plaintexts, the less evidential value will her refusal to decrypt have.

The other trade-off is more fundamental: *effectiveness versus the rule of law*. Using a refusal to decrypt as evidence is only possible in the few cases where there is already almost enough evidence (a *prima facie* case), and there is considerable evidence that the ciphertext at stake contains incriminating evidence that Alice is unwilling, although able, to decrypt. That is, if the current level of protection of the rights of the defense is to be maintained, the decryption command will not be very effective. To make it more effective would mean to cut down this protection, by shifting the burden of proof somewhat to the defense – more than the courts have allowed in recent case law. Here, the presumption of innocence is at stake; a real burden-of-proof shift does not seem to be compatible with the ECPHR.

Can one trade-off effectiveness with the rule of law? On the one hand, one can point out several cases in which the courts have allowed infringements of constitutional rights for criminal-political reasons – think of *Braswell* and *Murray*. On the other hand, one can argue that these cases have *explored* the borders of the rights at stake rather than *crossed* them; as I have indicated, *Braswell* is compatible with the rationale of the privilege against self-incrimination of providing reliable evidence, and *Murray* is compatible with the presumption of innocence.

I incline to defending the latter point of view. In current case law, the privilege against self-incrimination and the presumption of innocence have perhaps been narrowly interpreted, but their essence has remained intact. Were one to violate their essence, the constitutional courts would likely not tolerate this – the more so, as the effectiveness to be expected of an enforceable decryption command is not high anyway. If one is to maintain at least some respect for constitutional rights, notably the presumption of innocence, the same problem emerges which currently hampers the decryption command: how to show that Alice's ability to decrypt is a foregone conclusion? A *Garantenstellung* may help to prove this, but arguing that a particular suspect has vouched for the ability to decrypt by her person or former acts seems possible in a limited number of cases. Moreover, if one is to raise the potential punishment for refusing to cooperate, there must be more and stronger evidence in the primary case to meet the proportionality principle. And was not the evidence in the primary case insufficient *because* there was cryptography around? Here, we enter a vicious circle: Polly needs the plaintext to gain evidence that Alice committed a crime, and she needs evidence that Alice committed a crime in order to allow her to command Alice to decrypt and get the plaintext. That is not solving the problem. Creating a specific power that allows Polly to demand decryption, and enforce this with a penalization or a burden-of-proof shift, will not help her really more than her current ability to demand decryption if she can show that Alice is able to decrypt – a hard enough task for sure. In short, the effectiveness of this option can not be considered substantial.

In the Netherlands, Polly does not currently have this ability, and she will likely not get it in the (near) future, considering the removal of the proposed power to demand suspects to decrypt from the draft Computer Crime Act II. Interestingly, however, given the restrictions on the privilege against self-incrimination that the European Court seems to allow, the Dutch legislature *could* enact the withdrawn decryption-command proposal (overruling the current prohibitions to give a decryption command or a smart-card delivery command to suspects). To enforce the proposed provision, the legislature might consider allowing a burden-of-proof 'shift' when the police encounter a ciphertext, under strict Murray conditions. This may help to catch criminals, but if the presumption of innocence is to remain intact, the Murray conditions will be so severe that it will help in only few cases. In most cases, then, Polly will just have to leave the ciphertexts as they are, and look elsewhere.