Commanding Decryption and the Privilege Against Self-Incrimination

Bert-Jaap Koops[1]

Introduction[2]

Suppose you are a police officer on the brink of finding out who committed the murder you are investigating. You have probable cause to suspect someone, and you have his phone wiretapped. Unfortunately, when you listen to the taped conversations, you only hear gibberish. Did you intercept a fax message? No, it turns out that the suspect regularly scrambles his wire communications: he uses encryption to keep his conversations and computer messages secret. This, then, does not lead you any further.

Therefore, you decide to do a search at the suspect's place. There is no incriminating evidence readily at hand, but you have reason to believe that in the computer, incriminating messages may be stored, and perhaps also a diary. You browse eagerly in his computer, but when you click on the file diary.doc, the computer asks for your password for decryption. The file turns out to be encrypted – it looks like this:

```
qANQR1DBwU4DoFOjvEqaYQoQCADuZoWNo9hpUCugPFABqjbmsQwElkYgRxH5
Dm5Yh7seCQ1CG31AWkacOl/DVpmxpL7Og9nMiBmmucNg5BZn9kkrqT3qJhw7gbz
PtwsJ4WgP3KHx3A/Ep7+4BnZFCVc1sNlN4CpE7UiELWliee/R450+E+2y32lC/nKdgH
bzDw/HGL2lY88TV/+R4xQxr65/ECSCVGWtzZpAkkCaQwVdMQi2S7QZQNf3SLOIc
1RPWFftNH9xzIOGloyfOYWI/wwZmxHQeNIMuYt
```

So, what do you do? The only way to get that last bit of information you need to finalise the evidence, is to command the suspect to decrypt the scrambled files or to give you his password. But would this not force him to provide evidence against himself?

It is likely that a power to demand decryption is an infringement of the privilege against self-incrimination. Since this privilege is not absolute, the legislature could, in principle, decide to enact such a power. Is this justified? To what extent does the privilege against self-incrimination stretch? In this paper, I will deal with these questions, and suggest a way for legislatures to answer them. I will base my analysis on the situation in the Netherlands, and indicate the discussion in the United Kingdom, where these questions have been discussed on the basis of legislative proposals.[3]

[1] Dr. Bert-Jaap Koops is a senior research fellow with the Center for Law, Public Administration and Informatisation of Tilburg University, the Netherlands.

[2] This paper is based on research I conducted with a grant from the National Programme Information Technology and Law (ITeR). The text of this paper was finished on 1 January 2000. A more extensive study in Dutch will appear in the first half of 2000 in the ITeR series.

[3] For an analysis of the situation in US law, see Reitinger 1996 and Sergienko 1996.

The crypto controversy

Cryptography (secret writing), or crypto for short, is a means to hide data from unauthorised people. Since the 1970s, robust and reliable automated crypto systems provide efficient and generally uncrackable protection of communications and stored data. Since the mid-1990s, crypto programs have become user-friendlier and more widespread, and you can download several good programs from the Internet, such as Pretty Good Privacy.

To encrypt data, you need a crypto program and a key. For *de*crypting the data, you need the decryption key, which is the same as the *en*cryption key in "symmetric" cryptography (such as DES), or a *different* one in "asymmetric" or "public-key" cryptography (such as PGP). The decryption key (which is indeed key to keeping the data secret) must be kept secret, and is generally stored safely on a diskette or a hard disk, protected by a password.

More and more people are starting to use cryptography, and it is being built in in programs and the information infrastructure, because it is one of the best ways to provide information security – a requisite for electronic commerce. Since the middle of the 1990s, cryptography has proved itself an essential tool in the information society.

However, cryptography is not only used to safeguard e-commerce. Criminals are increasingly becoming aware of its potential to shield their incriminating information traffic from eavesdropping and computer-searching police. This has caused governments to think of ways to promote the good uses of cryptography and at the same time of preventing criminals from using it to thwart the police. This has turned out to be impossible. Whatever governments have come up with, such as requirements to store keys with third parties, has proved ineffective and unacceptable to the large majority of information citizens. My research into this issue has led me to the conclusion that the only way to really do something about the crypto problems for law enforcement, is to enact a power for the police to require suspects to decrypt.[4] Whether that is acceptable, in the light of the privilege against self-incrimination, is a complex issue, which requires careful study of the background of the privilege and of the pros and cons of such a power. So far, governments have been wary with infringing the privilege against self-incrimination for this purpose.

Current legal status of the decryption command

The Netherlands

During the Dutch parliamentary discussions over the Computer Crime Act (CCA), in 1992, the legislature became aware of the potential problems cryptography poses to law enforcement. They decided to introduce a power for the police to command someone to decrypt during a search. They respected, however, the privilege against self-incrimination, and so this command cannot be given to suspects (art. 125m DCCP). Then, in January 1998, a follow-up to the CCA was proposed, the Computer Crime Act II. This contained the power to demand people to decrypt data collected during a search or in a wiretap, and this time, the act proposed to also give this

[4] See my thesis, Koops 1998, in particular Chapter 8.

command to suspects, if there is grave evidence ("ernstige bezwaren") against the suspect and if this is urgently necessary for finding the truth. Several protests from the legal community were raised, and the Minister decided to withdraw the provision in the draft law that was submitted to Parliament in July 1999,[5] thus - again - respecting the privilege against self-incrimination.

The United Kingdom

In the UK, the government has been developing a crypto policy since 1996, with numerous consultation documents and proposals to regulate cryptography. Earlier versions of the policy were based on the idea that the crypto problem for law enforcement could be addressed by requiring people to deposit their keys with third parties. Given the many protests from UK citizens, and the intrinsic problems of such an approach, the government gradually moved to a position of voluntary key deposits and a requirement for people to decrypt when commanded by the police. This approach culminated in the consultation document *Building Confidence in Electronic Commerce* of 5 March 1999 and the subsequent E-Communications Bill. The consultation document proposed a power to require any person, upon service of a written notice, to produce plaintext or a decryption key (or password protecting a key). The ability to serve a written notice will be ancillary to powers for wiretapping or searching and seizing. According to the government, this power would not infringe the privilege against self-incrimination. To ensure compliance, the government would make it an offence not to comply with the terms of a written notice without reasonable excuse.

Then, on 23 July 1999, the government published a draft *Electronic Communications Bill*, together with a new consultation document *Promoting Electronic Commerce. Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report*, which also contains the Explanatory Notes to the draft Bill.

Article 10 of the draft bill contained a power to require disclosure of a crypto key. For encrypted material lawfully obtained, a written notice can be given to a person who appears to be in the possession of the key, to provide the encrypted information in intelligible form (that is, in the condition in which it was before any encryption or similar process was applied to it), or, if the notice explicitly orders so, to disclose the key. The notice needs to be authorised by the appropriate authority (depending on the powers under which the encrypted material was obtained), such as the Secretary of State, a judge, or a senior police officer.

Failing to comply with such a notice is an offence punishable with up to two years' imprisonment. It is a defence to show that you do not have the key, if you give sufficient information to enable possession of the key; likewise, it is a defence to show that it is not reasonably practicable to disclose the key, if you show that you provided it as soon as this was reasonably practicable.

This section of the EC Bill in particular caused a storm of protests, both from the ICT and the legal communities in the UK. The power was generally thought to breach the right to a fair trial as enshrined in article 6 of the European Convention of Human Rights.[6] The law-enforcement problems caused by cryptography were considered by far not serious enough to warrant the burden-of-proof reversal and the high punishment for not cooperating. The objections were

[5] Kamerstukken II 1998-1999, 26 671, nrs. 1-3.

[6] See, e.g., Beatson & Eicke 1999.

illustrated by a letter sent by the organisation Stand to Jack Straw, Home Secretary, containing an 'confession to a crime' encrypted with a key pair generated on Straw's name. The Metropolitan Police was informed that Straw was in possession of this information, and the keys were then destroyed by Stand. This way, Straw would be liable for two years in prison, unless he could prove that he did not know the key - which he could not, because Stand might have sent him a copy.[7]

After much protest, the government withdrew the contentious provision from the E-Communications Bill, in order to re-insert it in a Regulation of Investigatory Powers bill. The government was, however, still of the opinion that the power to demand decryption from suspects does not infringe art. 6 ECHR. As of January 2000, the discussions on the issue continue in the UK, and it is unclear what the outcome will be.

The privilege against self-incrimination

To be able to judge whether and to what extent a decryption command infringes the privilege against self-incrimination, and whether such an infringement is acceptable given the interests at stake, one must study the way the privilege has been interpreted and what infringements have been allowed to date. I will therefore first analyse the privilege, and subsequently give an overview of infringements that have been allowed in Dutch law.

The privilege against self-incrimination is a fundamental legal principle that is part of the right to a fair trial. It says that a suspect cannot be forced to incriminate himself or to yield evidence against himself. The privilege is recognised in most countries, either explicitly in the constitution or implicitly through case law. It is included explicitly in several international treaties, such as the International Covenant on Civil and Political Rights (article 14 para. 3 sub g: everyone charged with a criminal offence has the right not to be compelled to testify against himself or to confess guilt) and the Statute for the International Criminal Court (article 55 para 1 sub a: a person shall not be compelled to incriminate himself or herself or to confess guilt).

Moreover, the privilege is enshrined in article 6 of the European Convention of Human Rights, as interpreted by the European Court. The right to a fair trial incorporates "the right of anyone 'charged with a criminal offence', within the autonomous meaning of this expression in Art. 6,[8] to remain silent and not to contribute to incriminating himself."[9] In three cases,[10] the European Court has laid down the basis for determining the meaning of the privilege against self-

[7] Stand 1999.

[8] The "autonomous meaning" of the term "criminal charge" means that the European Court does not only look at the classification of the alleged offence in a nation's law (criminal or otherwise), but also at the nature of the offence and the nature of the penalty threatened.

[9] ECHR 25 February 1993 (*Funke v. France*).

[10] ECHR 25 February 1993 (*Funke v. France*), ECHR 17 December 1996 (*Saunders v. United Kingdom*) and ECHR 8 February 1996 (*Murray v. United Kingdom*).

incrimination, but at the same time, it has caused considerable confusion over this meaning. The *Saunders* case seems to give the most definitive statement about the privilege. 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.

There is not a general definition of the privilege against self-incrimination in Dutch law. The Constitution and the Dutch Code of Criminal Procedure (DCCP) do not mention it. The DCCP does contain several articles that reflect the privilege; for instance, a command to hand over goods or a command to provide access to a protected computer cannot be given to a suspect (art. 107 and art. 125m para. 1 DCCP).

The Dutch Supreme Court has initially said that "it would ill be in keeping with the spirit of the DCCP" if "the suspect would be compelled to contribute to his own conviction under threat of punishment",[11] but since 1977, it has often repeated the magic formula: "there is no unconditional right or principle that a suspect can not in any way be obliged to cooperate in the obtaining of possibly incriminating evidence".[12] The system of Dutch law indicates that, in general, suspects cannot be required to actively cooperate, but they do have to suffer acts that can incriminate them, such as the taking of blood samples. In special laws, dealing, e.g., with environment and tax crime, there are more compulsory powers for the police to require active cooperation from people, including suspects, such as handing over documents. An important reason for the difference between general and special criminal law is that, in the latter, cooperation requirements are considered necessary to find evidence at all that a crime as such has been committed. If people would be able to refuse to give tax documents to tax officials, tax crimes would not be discovered anymore, let alone prosecuted – so the argument goes.

From the European and Dutch interpretations of the privilege, one can conclude that although the privilege against self-incrimination is usually defined quite broadly ("not contribute to incriminating one-self"), the scope of the privilege is rather limited. It is a strong barrier to the compelled rendering of *testimonial* evidence, implying a suspect’s act or statement which somehow or other involves the use of his mind, but it is only a weak barrier to other means of compelled cooperation, such as suffering blood samples or handing over tax documents. In my understanding, the privilege does stretch to these kinds of "cooperation" as well (contrary to what the European Court in *Saunders* suggested) because the suspect cooperates in incriminating himself, but the privilege has a weaker impact on this kind of cooperation.

To understand why this is so, one should try to distil the rationale of the privilege from its history. People have suggested various reasons for the privilege.

1. Humanity: it is not humane to force someone to contribute to his own misfortune.
2. Autonomy: a suspect is free to choose an attitude in criminal proceedings, he can decide whether he wants to cooperate or not.
3. Reliability: evidence must be reliable.

[11] HR 16 January 1928, NJ 1928 p. 233.

[12] HR 15 February 1977, NJ 1977, 557 m.nt. GEM.

4. Prohibition of pressure: the privilege is a safeguard against the police using (too much) pressure to force a suspect to cooperate.

The third option has great explicative value. The disclosure of things which exist "outside of the will of the suspect" provides reliable evidence, whereas testimonial statements generally do not (you do not know whether the suspect tells the truth). Thus, the privilege contributes to truth-finding and shields the judiciary from "miscarriages of justice", as the European Court stated in *Murray*. However, I think it is impossible (and unnecessary) to pinpoint a single rationale: all of the above grounds have something to say for them and explain different aspects of the privilege.

One must realise that the privilege works on different levels. First, it is a principle the legislature has to take into account when introducing investigation powers. They cannot enact a power that unduly forces a suspect to incriminate himself. Here, the reliability rationale plays an important part: the more reliable evidence a power yields (such as breathalyser tests for drunk driving), the less strongly does the privilege work. And conversely, the less reliable a power is (such as requiring a suspect to make a statement on his involvement with the crime), the more strongly the privilege works.[13]

Second, the privilege has influence on the implementation of investigation powers. Here, it prevents the police from putting too much pressure on a suspect to cooperate when they use compulsory powers; this is the rationale of prohibition of pressure.

Third, the privilege plays a part in court. The court must decide whether information obtained through pressure on a suspect to cooperate is admissible as evidence. This is not a simple deduction from the wording of the law that allows investigation powers. Even if the police have the power to compel cooperation, such as handing over documents in a tax investigation, it does not follow automatically that the resulting data can be used as evidence. This can be illustrated by the *Saunders* case. The law that compels people to make statements is acceptable in light of the privilege – it targets people not charged with a criminal offence. However, in Saunders' case, the statements could not be used as evidence, because they had been used in the criminal proceedings in a way incompatible with the privilege. The privilege-infringing use of the statements was mainly caused by the influence the use of the documents had had on Saunders' attitude in court, particularly given the negative impression it created with the jury. Thus, the autonomy of the suspect and the prohibition of pressure are paramount in colouring the privilege as used in court, besides the reliability of the evidence.

Does a decryption command infringe the privilege?

From the definition of the privilege, it is clear that a decryption command is an infringement. Whether the suspect decrypts himself or whether he hands over a key and tells the password, in all cases, he actively cooperates in an activity that results directly in possibly incriminating evidence. Moreover, in most cases, the suspect will have to show or use the contents of his mind, because the password protecting the key is stored there. If the password is written down somewhere, the police can seize the paper or copy the password themselves; the decryption

[13] See Schalken's annotation of HR 29 October 1996, NJ 1997, 232.

command is targeted precisely at cases in which the password is not readily available to the police.

One can argue over the question to what extent telling a password is testimonial (in Dutch, a "verklaring"). On the one hand, it is not a statement concerning facts or circumstances - it is more like a physical key in that it either works or does not work. In that respect, the password is independent of the will of the suspect, because he cannot alter it with his will power. On the other hand, since the password exists in the mind (assuming the password is not written down somewhere), the suspect must operate his mind to reveal it. In that respect, the password has an existence which does depend upon his will, because if he refuses to give it (e.g., because he has forgotten it), the password, to all practical purposes, does not exist anymore. This means that, even if the password itself is not testimonial, the act of giving it will usually be testimonial: it reveals knowledge of the suspect. Only if it is a foregone conclusion that the suspect knows the password, can one hold that revealing the password is not testimonial.

This seems exactly the criterion that was pivotal to the *Funke* case, which the European Court decided in 1993. Funke was forced by French custom officials to hand over bank account documents "which they believed must exist, although they were not certain of the fact". Although the court decision is an obscure one, which has triggered divergent interpretations, I believe that this question whether the government knew or not that Funke had the power to comply was a crucial factor in deciding there had been an infringement of the privilege against self-incrimination. Because the officials were *not* sure that Funke had the documents, their forcing him to hand them over was incompatible with the privilege. After all, his refusal to comply could not lead to any conclusion: it may have been caused by unwillingness, but also by inability.[14]

In consequence, a decryption command is in all cases an infringement of the privilege against self-incrimination that prevents incriminating oneself, and it is also an infringement of the strong privilege that prevents providing testimonial evidence, if it is not a foregone conclusion that the suspect knows the password.

Precedents for infringing the privilege in Dutch law

Now, we are to decide whether a power to require suspects to decrypt is acceptable given the privilege and the other interests at stake. This primarily concerns the first level on which the privilege operates: that of the legislature. In balancing the interests at stake, the legislature must bear in mind the system of the law and the arguments one can use to infringe fundamental rights. Therefore, one must analyse what laws the legislature has passed until now to allow infringements. For brevity's sake, I restrict myself to the Dutch situation.

[14] For this interpretation of *Funke* and the related case of *Fisher v. United States*, see Koops 1998, p. 175. The same interpretation is given by Rozemond 1998, p. 316. See also the recent certiorari granted by the Supreme Court in *United States v. Hubbell* (D.C. Cir., 167 F.3d 552): the Fifth Amendment protects the production of business and financial records, unless the government can show its prior knowledge of the information.

First, several laws require people to make testimonial statements. There are reporting requirements: e.g., doctors carrying out euthanasia, farmers dealing with manure, and financial institutions accepting unusual amounts of money all have to file reports. These can lead the Public Prosecutor to start an investigation, if the report suggests that rules have not been complied with. Generally, the information contained in the reports can be used as evidence in a criminal trial, because the reporting law addresses non-suspects in regulatory, not criminal, affairs. In certain laws, however, an exception has been made: the law requiring the reporting of unusual financial transactions stipulates that the information cannot be used in a prosecution of financial institutions for receiving (“heling”). This is because the law is targeted at catching money-laundering criminals, not the reporting financial institutions.

Then, in several special laws, there are requirements to provide information, e.g., in supervisory activities concerning taxes, drugs, or weapons. Usually, the supervisory officials can require people to provide information, but if the addressee is a suspect, he can refuse to testify. This is not so in the Law on Weapons and Munitions: if a suspect does not comply with an order to provide information, he can be fined. This exception may be explained by the importance of controlling the risk of weapons, the restricted scope of the law, and the low punishment, leading to the infringement of the privilege against self-incrimination to be acceptable to the legislature.

Then, witnesses usually are obliged to speak. In criminal cases, however, they can refuse to answer a question if in answering they would incriminate themselves. In parliamentary inquests, they cannot refuse to speak, but a special provision forbids using their answers as evidence in criminal cases. Thus, there are different levels of self-incrimination protection: suspects never have to answer, witnesses in criminal cases can only refuse to answer certain questions, and witnesses in parliamentary inquests always have to answer, but resulting evidence is inadmissible.

A special case is car registration-number liability. The holder of a registration number is liable for certain offences committed with the car, unless he tells the police who was the driver. If he fails to indicate the driver, the registration-number holder can be sentenced to the same punishment as can be given for the offence at issue. Thus, in fact, people are forced to give information, and a refusal is penalised. This infringement of the privilege against self-incrimination should be explained by the special circumstances of the Road Traffic Act, where car owners are considered to have a responsibility to prevent others to use their cars to endanger road safety with impunity. Still, it is the only case in Dutch law where suspects can be forced to make a statement (the name and full address of the driver) while a refusal to comply is punishable with a prison sentence. As such, it hardly fits in with the way Dutch law has incorporated the privilege against self-incrimination.

The general conclusion must be that suspects can, in principle, never be forced to make statements. People who are not a suspect, however, can be forced to give testimonial evidence, although they can usually refuse to comply if they would incriminate themselves. Generally, resulting evidence may not be used against them in court. It is only in very few, restricted areas (weapons, traffic) that compelled statements may be admissible as evidence.

Second, there are requirements to force suspects to actively cooperate with the police – a broader class of cooperation, and less contentious than providing testimonial evidence because the right to silence need not be at stake. One can think of the many requirements in special laws to hand over documents or things that may be helpful for uncovering the truth. Also, in traffic law, people suspected of drunk driving have to actively cooperate with a blood or breath test. If suspects refuse to cooperate, they can be punished with a prison sentence (in tax law), or with the same punishment as can be given for drunk driving (in traffic law). Here, therefore, we see that the privilege is infringed, but that the legislature has allowed this infringement after a balancing of the interests at stake. In these cases, the privilege against self-incrimination has less weight because it concerns material independent of the will of the accused. Thus, the necessities of enforcing special laws (regulating specific kinds of economic activities) can be considered to outweigh the privilege. Further arguments for this balance are the relatively low punishments (in the special laws) and the subsidiarity principle, which holds that a compulsory power which breaches fundamental rights is more acceptable if there are no other powers available to achieve the goals of the legislation (which is a particularly valid argument in the traffic law, because drunk driving can hardly be proved otherwise).

This overview leads to the conclusion that, in general criminal law, suspects do not have to cooperate. In special laws, they often have to actively cooperate, but they usually cannot be forced to give testimonial evidence. Infringements of the privilege against self-incrimination are allowed more easily in special laws, largely because of the principle of subsidiarity (it is harder to prosecute crime in economic-activity regulating areas, because the crime is usually more covert) and because of the principle of proportionality (the more restricted the scope of the law, the less an infringement forced cooperation is).

Furthermore, the laws show different ways of incorporating the privilege against self-incrimination: sometimes, people cannot be forced to cooperate; sometimes, they can be addressed with a cooperation command but they can refuse to comply; sometimes, they are obliged to comply, but resulting data cannot be used as evidence against them at all; and sometimes, people are obliged to cooperate, but resulting evidence is inadmissible in court under certain circumstances. Only laws of the last category concern true infringements of the privilege against self-incrimination.

Options for commanding decryption

Now, if we look at the issue at hand, the analysis of precedents suggests various ways of enacting a decryption command within - and outside of - the limits of the privilege against self-incrimination. I present these in order of increasing infringement of the privilege against self-incrimination.

1. A decryption command that cannot be given to suspects.
2. A decryption command to all persons. People can refuse if by complying they would incriminate themselves.
3. A decryption command to all persons. Suspects have to comply. Resulting data cannot be used for investigation.
4. A decryption command to all persons. Suspects have to comply. Resulting data cannot be used as evidence.
5. A decryption command to all persons. Suspects have to comply. Resulting data

- *can* be used as evidence only if certain conditions apply; or
- *cannot* be used as evidence only if certain conditions apply.

6. A decryption command to all persons. Suspects have to comply. Resulting data can be used as evidence.

Moreover, these options can be chosen for

A. criminal law in general (the Code of Criminal Procedure), or
B. only specific laws (such as tax law, environment law, or drugs law).

To ensure effectiveness, one can choose various enforcement options. A refusal to comply with a decryption command:

i. is punishable as not complying with a legal order (like art. 184 DCC, maximum three months' imprisonment);

ii. is punishable in its own right, with a specific maximum punishment that
- is the same for all crimes; or
- is somehow tied to the crime being investigated;

iii. can be used as evidence by drawing an adverse inference in the case against the addressee.

In all options, variables can be added to limit the scope of the power (and the consequent infringement), such as restricting the power to serious crimes, a requirement of probable cause ("redelijke verdenking") or of grave evidence ("ernstige bezwaren"), and requirements of urgency and necessity.

As Dutch law currently stands, A1i is the case.[15] The issue in the Netherlands, then, is to what extent a "heavier" law can and should be established, where A6 is the most far-reaching.

Enforcement and ability to decrypt

One of the major factors in the decision to introduce a decryption-order law targeted at suspects is enforcement. After all, if the order is to be effective, there must be a threat of punishment for not complying. Such a punishment can only be given to people who *wilfully* do not comply. Otherwise, a risk liability would be introduced for encryption use: if you ever find yourself in front of the police asking you to decrypt, you have to comply, whether or not you are able to. That is unacceptable, given the importance of cryptography in the information society and the fact that using encryption is in no way of itself a dangerous activity. Therefore, if someone is to be punished for not decrypting, the police will have to show that he was able to decrypt.

Here, problems emerge. Addressees can generally easily hide unwillingness to cooperate under retorts of “I forgot my password”, “These random data must have been copied to my computer

[15] In various special laws, requirements to cooperate can be interpreted as including a command to decrypt, like the requirement in tax law to show books, which must be presented in an understandable format; these could be seen as decryption commands of the type B2ii and B3ii (and B6ii in the case of the munitions law requirement to cooperate).

when I downloaded something from the Internet - I've no idea what they are", and "I haven't used that decryption key for over a year".[16] Especially the retort that the addressee forgot his password is difficult to refute. The police can give arguments why someone should be able to remember his password (e.g., because he is a professional crypto user who has never forgotten his password at the office), but there are too many arguments the suspect can give to make this unlikely (e.g., "I used a particularly difficult password, as my crypto consultant advised me, which I was not allowed to write down - and I haven't used it that often").
Moreover, calculating criminals have plenty of opportunities to anticipate a decryption order. For instance, they can remove all header information so that one cannot see whether the file is encrypted or just consists of random data, they can often change key pairs, and they can antedate files in their computers so that they can argue that they no longer remember the key with which it was encrypted long ago. Also, the crypto community will devise robust schemes for "perfect forward secrecy", in which it is not possible for the user to decrypt the data after a certain period. As a result, a decryption order will be particularly powerless against calculating criminals, while less-calculating criminals can benefit from an I-forgot-my-password retort. Therefore, it will hardly be useful to put a significant punishment on not complying with a decryption order - the prosecution will have too hard a task to show that someone wilfully did not comply.

Choosing an option

In the scope of this article, I cannot provide a definitive answer to the question what kind of decryption command the Dutch or UK legislatures should choose. This, after all, is a question which requires thorough analysis of several issues, as well as a political balancing of interests. Rather, I shall indicate the procedure legislatures have to follow to be able to make a justified and reasonable choice.

To introduce a decryption command that balances the interests of crime-fighting and the right to a fair trial, the legislature must analyse the following.

1. What is the **scope of the privilege** against self-incrimination in their law system? I have indicated this for the Dutch situation above.
2. What **kind of crimes** is at stake in which the investigation is hampered by encryption? Are these numerous, more general crimes, or mainly certain specific crimes? How serious are these crimes? This analysis should be based on empirical studies of investigation practice.[17] My current impression is that cryptography has truly obstructed investigation in only very few cases to date, although this may change significantly if cryptography is built in in mass-market software, such as operating systems and mail programs.
3. **How** does cryptography hamper investigation? Does it mainly hamper the (initial stages of) investigation (notably in wiretaps), making it more difficult to find out who may be involved

[16] See Koops 1999, section 4, for an overview of these technical issues.

[17] Denning & Baugh 1997 have initiated such an empirical study, but this was rather preliminary and ad hoc. No data avail for the Netherlands. Governments should stimulate studies of the extent to which investigation is hampered by cryptography, rather than roughly indicate the theoretical problems.

in the crime, or does it obstruct the stage of prosecution, making it difficult to finalise the evidence (notably in computer searches)?

4. What **alternatives** are there to investigate and gather sufficient evidence? Does this depend on the kind of crime and investigation involved? E.g., it may be the case that in general investigation, there are sufficient other alternatives (such as infiltration, or using directional microphones and bugs), whereas in specific supervision procedures and investigations (such as tax and environment law), there are far less viable alternatives. Here, one must also assess the extent to which the alternatives infringe fundamental rights, such as the right to privacy and the right to a fair trial, in order to assess what is the least burdensome power.
5. If a power to demand decryption is found necessary, what **safeguards** should be in place to make it as little infringing as possible within the limits of effectiveness? Here, one must choose conditions of the seriousness of the crimes for which the power can be exerted, the amount of suspicion against the addressee, the likelihood of the encrypted data at issue to be useful or necessary for the investigation, and the like. The legislature should look at comparable investigation powers to make the decryption command neatly fit in with the system of the law. Moreover, a safeguard should be built-in to prevent keys used for digital signatures to be handed over.
6. What kind of **enforcement** is required? Here, the legislature must choose between the general penalisation of not complying with a legal order, a specific penalisation for not complying with this order - with an appropriate and just maximum punishment, and a provision that allows the judge to draw an adverse inference from a refusal to comply (effectively reversing the burden of proof for the incriminating nature of the encrypted data). Generally, the enforcement will not be effective given the ease with which addressees can claim not to be able to comply. This is a strong argument against a severe infringement of the privilege against self-incrimination.

Conclusion

Cryptography is a potential problem for law enforcement, hampering wiretaps and computer searches. The only way to really solve this problem would be to force suspects to decrypt, but this infringes the privilege against self-incrimination. Governments can decide to introduce a power to command suspects to decrypt, if a full analysis of the problems in practice and the system of the law lead them to account more weight to the necessity of fighting crime than to the privilege against self-incrimination in this particular respect. It is likely, however, that such a power will not be effective if targeted at suspects. As a result, there should be the most serious and compelling arguments to introduce a decryption power to suspects nonetheless - such as the fact that cryptography is definitively blocking a large number of prosecutions of serious crimes, in which there is no alternative but to get the key to decrypt possibly incriminating evidence. At present, this is far from the case, and it is unlikely that such will ever be the case.
Therefore, an infringement of the privilege against self-incrimination is not warranted. The current Dutch provision that a decryption order can not be given to suspects is a sound one.

References

Beatson & Eicke 1999

Jack Beatson and Tim Eicke, 'In the matter of the draft Electronic Communications Bill and in the matter of a human rights audit for Justice and FIPR', 7 October 1999, WWW <http://www.fipr.org/ecomm99/ecommaud.html>

Denning & Baugh 1997

Dorothy Denning, William Baugh, *Cases involving encryption in crime and terrorism*, version 10 October 1997, <http://www.cs.georgetown.edu/~denning/crypto/cases.html>

Koops 1998

B.J. Koops, *The Crypto Controversy. A Key Conflict in the Information Society*, The Hague: Kluwer Law International 1998

Koops 1999

Bert-Jaap Koops, *Crypto and Self-Incrimination FAQ*, version 1.1, 13 August 1999, WWW <http://cwis.kub.nl/~frw/people/koops/casi-faq.htm>

Reitinger 1996

Phillip R. Reitinger, 'Compelled Production of Plaintext and Keys', *University of Chicago Legal Forum* 1996, p. 171-206

Rozemond 1998

Klaas Rozemond, *Strafvorderlijke rechtsvinding*, Deventer: Gouda Quint 1998

Schalken 1996

Tom Schalken, annotation of HR 29 October 1996, NJ 1997, 232, m.nt. Sch.

Sergienko 1996

Greg Sergienko, 'Self Incrimination and Cryptographic Keys', *Richmond Journal of Law & Technology*, No. 1 (1996), WWW <http://www.urich.edu/~jolt/v2i1/sergienko.html>

Stand 1999

Malcolm Hutty, Stand.org.uk, 'Letter to Jack Straw, Home Secretary', WWW <http://www.stand.org.uk/dearjack/>, no date (accessed 24 November 1999)