

Chapter 9. Alternative investigation measures

*You read the clicking keys as gibberish
Although they strike out sentences to sense.
So in the fluttering leaves, the shoaling fish,
The continuum nondenumerable and dense,
Dame Kind keeps rattling off her evidence.
(Howard Nemerov, Analogue)*

If the police want to read encrypted data, they can either crack them or try and get the key. Cracking, as pointed out in Chapter 4, will be difficult and, in many cases, impossible. Accessing the key will then be the only option. However, Chapters 7 and 8 show that accessing the key beforehand (through LEAKing) or afterwards (through demanding decryption) is wrought with problems. Perhaps, then, the police will just have to leave the encrypted data as they are – unreadable, unfathomable, beyond access.

Rather than sit down and despond over the hardships of modern crime fighting, the police can move on and try other ways of finding information on crime and criminals. After all, wiretapping and computer searches are not the only ways to catch criminals. If modern technology hampers their work, why could it not help the police in other ways? Directional microphones have become strong enough to listen in on conversations taking place hundreds of meters away in a building, and bugs prove a good way of direct eavesdropping.¹ Electromagnetic radiation from a computer screen can be tapped from a house next-door.

Moreover, other legal investigation measures may be considered. The police can infiltrate a criminal network, and gather first-hand information in person. Or, if suspect Alice refuses to decrypt, why not ask accomplice Bob to testify against her in return for some impunity? Ultimately, if no new sources of information can be found, the police can re-examine the data they already have; here, data-warehousing and data-mining techniques may help in ordering the overwhelming amounts of information that roam around in police files – and in the public domain – to find information needles in data haystacks.

Of course, such investigation measures are disputed – even if they are technically feasible, there are major legal obstacles to overcome: such measures threaten people’s privacy and the rule of law, and Big Brother looms large on the horizon of extended observational investigation measures.

This chapter deals with such alternatives to wiretapping and computer searches. I use

¹ Note that in the US understanding, ‘wiretapping’ covers intercepting (voice and electronic) telecommunications as well as bugging (‘oral interception’). In the Netherlands, wiretapping only covers intercepting telecommunications. Bugging, or, more general, oral interception, has until now not been allowed for law enforcement. Therefore, it is a topic in this chapter as an alternative investigation measure.

‘alternative’ in the sense of ‘another way’ to gather information, possibly as a supplement, rather than as a strict replacement of wiretaps or computer searches. Of course, there are many ways to gather information. In this chapter, I describe five measures which may to some extent serve to fill the information gap caused by cryptocriminals. There are doubtless other measures that can function as supplementary sources of information; the five measures described here serve as examples of ways in which to look for other powers:

- *technical* measures that are *closely related* to wiretaps and computer searches (direct eavesdropping (9.1) and intercepting electromagnetic radiation (9.2));
- *legal* measures to gather information on criminal organizations (infiltration (9.3) and crown witnesses (9.4)); these are *further removed* from wiretaps and computer searches but may provide similarly useful information in organized crime cases; and
- a *technical* measure dealing with information management in general, *unrelated* to wiretaps and computer searches (data mining (9.5)).

For each measure, I shall indicate in what situations it may be useful, what sorts of crimes may be involved, and what is its relation to cryptography, in order to assess to what extent it may be regarded as an ‘alternative’ to tapping or searching. For every measure, I will describe the legal issues involved: is it currently allowed or being considered, or is it imaginable in light of the investigational culture? I will conclude with a definition of what alternative investigation measures may be considered options to address the crypto conflict, and assess how they relate to the principles (9.6).

As this chapter is meant as a source for inspiration rather than a final, exhaustive analysis of investigation measures, it touches upon the legal issues involved and is not an in-depth analysis. Its main intention is to show that there are other ways of investigating, if tapping and searching computers are rendered useless through encryption.

Like in Chapter 4, the analysis in this chapter focuses on the Dutch situation when it comes to assessing whether a particular measure can be considered viable – after all, this depends to a large extent on the national culture of criminal investigation. For other countries, the assessment may yield a different result; therefore, I will include some information on the situation in other countries.

9.1. ‘Direct eavesdropping’

“The antennae!” said Legrand, who seemed to be getting unaccountably warm upon the subject; “I am sure you must see the antennae.”
(Edgar Allan Poe, *The Gold-Bug*)

Before Alexander Bell, people only talked to each other in person (well, sometimes through tom-toms, smoke signals, or optical telegraphs), and the police could only listen in on them by standing close to them. With the advent of (long-)distance communications, people increasingly converse without seeing each other – or the police who is listening in. In fact, with the telephone, the police gained an eavesdropping method which was safer and more secure than before. Now that encryption hampers eavesdropping in between, the police may

have to resort to the old method of listening in: at the edge, near one of the telecommunicating partners, or directly at 'face-mail' conversations.

9.1.1. Description

'Direct eavesdropping' is the monitoring and recording of communications with technical means – directly where the communication takes place.² One can distinguish three types:

1. listening in on and recording a conversation in its direct presence;
2. listening in on and recording with a directional microphone;
3. placing bugs.

The borders between the types are fuzzy, but there is a clear difference in practicality.

Recording a conversation *directly* is quite feasible when it is done by one of the interlocutors (consensual monitoring). By carrying a small tape recorder in one's pocket, one can record conversations in public or, more interesting still, in private. This has been done several times by informants or undercover agents. [Traa, 175] Recording a conversation may also occur in public, for instance, near people sipping a beer on a terrace, or talking on the corner of the street. A (plainclothes) policeman sitting near the suspect(s) can record the

conversation at the next table with a device he carries in a suitcase or briefcase. In practice, for the time being, it seems to be of little value, according to W.J.A. Paulissen, former leader of the Core Team South: "If you're there, you catch snippets of a conversation at an adjacent table. Why not try as a policeman to catch those snippets? (...) Looking back, it all looks rather amateurish. It didn't work, then. So, at a given point, we stopped." [Traa, 176]

Directional microphones are more stealthy. They are potentially strong enough to overhear conversations at a distance of several hundreds of meters,

even across walls; often, however, there is too much background noise to distinguish anything useful. "I have never seen such a thing work. They have never been able to prove to me that this is doable for our kind of work. It is nice in a forest, when it's very quiet, for the birds, but I don't think you can use a directional microphone in a city like Amsterdam." [A. Kloosterman, observation detective, in Traa, 177] Indeed, paranoid criminals may employ disrupting devices to thwart this kind of eavesdropping: "It appears from recent press releases that some professional criminals protect themselves from directional microphones with an 'acoustic

2 The Dutch legislature uses a slightly different classification. It describes the power to record confidential communication with technical means, which apart from bugs and directional microphones, also covers scanners.

noise generator': a small box that fills the room with electronic noise that thwarts all eavesdropping techniques." [23047, nr 5, 8] On the other hand, given the fact that many criminals speak in hardly disguised language over the phone, even while they can expect being wiretapped, many criminals will not take precautions. A study on interception in the US found that in 80 per cent of the cases involving direct eavesdropping, incriminating conversations were recorded. "The experts consulted by us on this point confirmed this estimation [that criminals only seldomly take precautions against eavesdropping], and added that a large part of the people arrested had, also according to their own statements, felt absolutely secure." [Böttger, 14] Through their size, directional microphones can only be used in certain circumstances, when they can be placed stealthily somewhere next-door or in a car – they are not the kind of device you carry with you in the street.

Placing *bugs* may be more useful; experience in the US shows that it is a valuable way to gather information [Böttger]; think of what people may say in a parlor or a sleeping room. Bugs can transmit or record conversations quite clearly (for instance, when placed in a telephone, a lamp, or a cockroach), and they can also transmit or record computer activity (keyboard strokes and mouse clicks). Placing bugs requires breaking into the suspect's premises to place them, and so, there is a risk of being discovered and alarming the suspect.

9.1.2. Situations, crimes, and encryption

Direct eavesdropping centers on overhearing conversations. It is a measure directed at communications, both in person and through telecommunications. Thus, it is especially relevant to investigating criminal organizations, who have a high communication need (see 4.1.1). The police can use it to quickly gain knowledge on how the organization functions and who are involved. It will therefore be important in the early investigation stage. The initial Dutch law proposal from 1993 on direct eavesdropping specifically introduced a 'proactive' stage as a focus for direct eavesdropping. Indeed, the reason why direct eavesdropping was proposed, was the "increase in serious crime, the hidden way in which it functions and the technological developments, through which especially organized crime is able to communicate without using the public telephone, and thus out of reach of the telephone tap. Intensive communication is of great importance for these kinds of crime." [23047, nr 6, 9]

Also in other forms of serious, 'non-organized' crime, direct eavesdropping may be relevant [23047, nr 12, 8]. It was (illegally) used, for instance, in the investigation of a violent murder. A drug addict who lived at his mother's was suspected. During two days, their conversations were recorded from the house next-door, from which it appeared that the boy was not involved in the murder. [Traa, 176] Bugging, for which locations have to be entered to place bugs without the owner's consent, can be considered in offices, as well as in houses and cars of (serious) organized criminals. Bugging may therefore be especially relevant to investigating organized crime and business crime.

However, not only conversations can be recorded, but also keyboard strokes. Thus, e-mail messages, passwords, letters, private notes et cetera can be recorded. Although keyboard strokes are not directly interpretable, it is possible to derive the contents of someone's typing activity after close scrutiny of someone's typing pattern in one or two days (it helps if you

know the language being typed). Thus, one might transcribe keyboard strokes if enough strokes are captured. One should not overestimate this possibility, though. It requires the recording of many key strokes, intensive study of the pattern, and therefore is very resource-consuming. Moreover, with the increasing use of Windows programs and the consequent increasing use of the mouse, investigating keyboard strokes may become increasingly difficult (I estimate that retracing and interpreting mouse movements is harder than interpreting keyboard strokes). Still, in some cases, bugging the keyboard can yield plaintext of messages or files before encryption; it may even yield passwords that protect encryption keys (most encryption programs store private keys on a hard disk or chip card with password protection).

Contrary to wiretapping, direct eavesdropping is not hampered by cryptography. Indeed, where end-to-end cryptography hampers wiretapping because it takes place *between* the two ends, direct eavesdropping takes place *at* one end, before the speech is being encrypted (or after it is decrypted). This was one of the main reasons for the Minister of Justice in 1993 to propose direct eavesdropping as an investigation measure: “The increase in serious crime, together with the more hidden way in which it operates, necessitates submitting this proposal. What is more, also the technological developments unfortunately urge this. (...) Already at this moment, and certainly in the near future, the technological developments allow entertaining communication out of reach from the judiciary and police. The possibility to have advanced cryptology is an example of this. The competence now proposed can to a certain extent serve as a replacement for the decreasing possibilities to intercept telecommunications.” [23047, nr 3, 2-3]

In all, direct eavesdropping is a good alternative to wiretapping.³ It yields the same kind of information (people’s conversations), albeit in somewhat different circumstances: it focuses on personal conversations in private or public. Telecommunication may also be recorded, which will yield only one half of the conversation, but this need not be a serious drawback. However, direct eavesdropping can not replace the wiretapping of facsimile or e-mail messages; it is only a logical alternative to wiretapping conversations. Given the difficulty of interpreting recorded keyboard strokes, and, what is more, the fact that computers contain a lot more information than what is typed in the interception period, it is less effective an alternative to the search and seizure of stored information.

9.1.3. Legal status in the Netherlands

Direct eavesdropping is currently not allowed for law enforcement, but it will likely be in the near future when the draft law on special investigation powers is enacted (it is, incidentally, already legal for the Dutch National Security Service). Despite its being illegal, the police has used direct eavesdropping several times a year. [Traa, 329]

With the introduction of the power to tap phones in the late 1960s, direct eavesdropping for law enforcement was also discussed. At the time, it was considered too grave an

3 Indeed, some investigating officials have noticed a shift in criminals’ communication behavior: “We saw that criminals didn’t talk over the phone with each other, but traveled all over the country to meet each other. We even had a case in which someone traveled to Luxemburg to chat with someone on the corner for ten minutes, and then returned.” [W.J.A. Paulissen, former team leader Core Team South, quoted in Traa, 175]

infringement of privacy. The Explanatory Memorandum to the tap law explicitly stated, however, that the result of the balance of interests involved could shift due to an increase in, particularly, serious and organized crime [23047, nr 3, 1-2]. Apparently, by the early 1990s, the time had come to rebalance the interests, and the proposal to allow direct eavesdropping was submitted: the developments in serious and organized crime and in cryptographic technologies were now seen to necessitate the measure. The parliament took its time discussing the proposal, and with a view to the discussion on investigation methods resulting from IRT-gate, the proposal got stuck somewhere in the First Chamber.

In 1997, it was reintroduced in the draft law on special investigation methods [25403, nrs 1-2]. This law allows the recording of confidential communications with a technical device. The power may be used when there is probable cause of a crime which allows pre-trial detention and which forms a serious threat to the legal order. Moreover, it must reasonably be necessary for the investigation. There is no requirement that the suspect should be a participant to the communication. The placing of bugs is allowed in non-public places; there are stricter conditions for placing bugs or otherwise recording communication within homes. The order for recording communications requires a warrant of the examining judge; it can be given for a period of four weeks, and can be extended every four weeks. Undercover agents recording conversations in which they themselves participate also require a warrant, although it is considered less privacy-infringing (the suspect should be aware of the possibility of talking to an undercover agent, and so, he has less expectation of privacy than is the case with stealth recording through bugs or directional microphones). The same power is allowed when there is not (yet) probable cause for suspecting someone of a specific crime, but when there is a reasonable presumption that he is involved in the scheming or committing of organized crimes.⁴ In this case, only communications in which the person involved (the 'suspect') participates may be recorded.

The law pays specific attention to the evidentiary value of recorded conversations. Since the recording (in case of a bug) takes place outside the view of the police, there should be guarantees that the recordings cannot be hampered with. Moreover, background noise has to be filtered out, and so, the tapes have to be upgraded by specialists. This entire process has to be auditable to allow the defense to challenge the evidence. Specific procedures and technical requirements, to be outlined in an Order in Council, will see to it that the process of recording and upgrading is done in a transparent, verifiable way.

The term confidential communications indicates the private exchange of messages between two or more persons, for instance, a private conversation, a private e-mail message, non-public radio traffic, and even the use of an ATM; it does not, however, cover entering data in a personal computer. Therefore, if it is expected that a computer is not used for communication (notably, if the computer is not attached to a network), direct eavesdropping is not allowed. Still, it may incidentally happen that a bug records data (typing a personal

4 The Minister of Justice abandoned the 'proactive stage' approach of the earlier proposal. In her opinion, the stage in which you suspect someone of scheming or committing organized crimes and the stage in which you suspect someone of a specific crime overlap. It is the focus of the investigation (organized crime versus investigation of a specific crime) which matters, not the various stages, which are chronologically diffuse.

letter, talking in oneself, dictating a letter) at which the power is not targeted; the Explanatory Memorandum is not clear whether such data can be used as evidence or not. [25403, nr 3, 35-6]

With the possible exception of undercover agents recording conversations, direct eavesdropping is an extremely privacy-infringing measure. Especially in homes, people expect complete privacy – it is the only place where one can be completely oneself, and where one can rely on not being intruded upon. Whereas the 1993 Dutch proposal for direct eavesdropping allowed bugging in homes (under severe restrictions [23047, nr 3, 7]), the draft law on special investigation powers initially ruled out eavesdropping in homes. The Minister of Justice considered the privacy within homes to be too sacred. However, after criticism from the police, the Council of State, and Parliament on the dubious effectiveness of the measure if it were not allowed in homes, the Minister granted the power to eavesdrop in homes if this is necessary for the investigation of a crime that is punishable with at least eight years [25403, nr 8].⁵

9.1.4. Situation in other countries

In *Germany*, direct eavesdropping is allowed to a certain extent. The German states allow preventive eavesdropping to avert danger; the preconditions for this differ per state [see Kutscha]. Although this power is limited to prevention, the German Federal Court has decided, in a controversial case, that information gathered from preventive eavesdropping can be used for a criminal investigation [*NJW* 1996, 405].

There has been a heated debate in Germany to what extent direct eavesdropping can be used for criminal investigation [see, e.g., Seifert, Ostendorf]. Germany distinguishes between ‘small’ oral interception (recording of a conversation by an undercover agent) and ‘big’ oral interception (bugs and directional microphones). With the *Law to Fight Drug Dealing and Other Forms of Organized Crime* of July 1992, a power was introduced to intercept and record not-publicly spoken words with technical means. The conditions are similar to the conditions for tapping phones, and it can be used only if other measures are useless or considerably more difficult. Although this indicates a broad power, it excludes eavesdropping within houses, as this was rejected in an earlier draft. It was generally accepted that the German constitution would have to be amended to allow direct eavesdropping in houses. In 1997, the debate started anew with the draft *Act on improving the fight against organized crime*. The law was enacted in May 1998, allowing direct eavesdropping in homes, after the constitution had been amended to that effect in March.

In the *United States*, bugging is a common practice. A survey of interception in the US between 1987 and 1992 [Böttger] found bugging to have been used in 567 of 4,935 cases involving interceptions (11,5 per cent).⁶ Much more than wiretaps, bugging took place in offices (40.4 per cent); 18.6 per cent involved bugging in houses, and 38.7 per cent elsewhere (cars, hotel rooms, and others); compare this to wiretaps, which involved houses in 66.9 per

5 MP Vos has proposed an amendment to lower this to five years, since she considers direct eavesdropping within homes to be preferable over infiltration.

6 The survey split the cases in wiretap, bugging, electronic communications, and combinations thereof. In the following, I mention the figures for wiretap only and bugging only, in order to show the differences between the two.

cent, 14.9 per cent in offices, and 11.5 per cent elsewhere. Bugging yielded more irrelevant conversations than wiretaps (7.2 per cent of the conversations were incriminating in bugging, 20.5 per cent in wiretaps), but it involved far less people being overheard (26.5 persons per bugging case, versus 138.1 persons per wiretap case). Therefore, bugging is in some respects less privacy-infringing than wiretaps (less people are overheard, relatively often in offices), but more so in other respects (more irrelevant private conversations are recorded, and people have a higher expectation of privacy when talking in private than when talking over the phone).

As to its efficacy, bugging yielded incriminating conversations in 80.9 per cent of the cases (95.3 per cent with wiretaps), but the percentage of cases which led to arrests or convictions is much lower: 29.6 per cent arrests and 20.4 per cent convictions (compared to 46.7 per cent arrests and 33.1 per cent convictions with wiretaps). Despite these relatively low figures, it did turn out that once an interception led to an arrest, many more arrests or convictions followed (8 to 15 on average), which indicates that wiretaps and direct eavesdropping are especially efficacious measures for prosecuting (organized) groups. Setting off the number of people being overheard against the number of convictions, the ratio for bugging (17.1:1) is more favorable than wiretapping (44.7:1) or the combined use of wiretaps and bugs (77.5:1), but it is apparently somewhat less effective than wiretaps.

The survey concluded that bugging is only seldom authorized by judges in the US. It gave as reasons for this the fact that trespassing to place a bug constitutes a significant risk, that a specially high percentage of irrelevant small-talk is overheard (which makes it time-consuming), that the bugs can be discovered, and that judges are required to authorize only the least privacy-infringing measure.

9.1.5. Conclusion

Direct eavesdropping is to a certain extent a good alternative to wiretapping, particularly as it is not hampered by encryption; it will likely soon be introduced in Dutch law. In particular, undercover agents can record conversations, and directional microphones may be used to a certain extent, although they are technically not always usable, and they may only be used to eavesdrop on in-house conversations in very grave cases. Bugging seems to be the best option – the US survey shows that it is a serious alternative to wiretapping telecommunications. However, although in some ways less privacy-infringing than wiretapping, bugging is in many ways a grave infringement of people's privacy; for that reason, in the Netherlands, it will only be possible in houses in the investigation of the most serious crimes, contrary to the US. Overall, bugging is less efficient than wiretapping in general: it can not record facsimile messages, and, given the risks of detection and its being time-consuming to sift out all the small-talk, will have to be used more sparingly. Still, it yields the same kind of information as wiretapping, which makes it the most direct alternative to record criminal conversations.

9.2. Tempest monitoring

Brave new world
(*Shakespeare, The Tempest*)

Computers can do more than you think – they may even do more than you want. Computer screens allow you to see what you do, but they also emit radiation which allows others to see the same. This ‘gift’ of free electromagnetic radiation is a feature of all computer screens and peripherals, although the intensity (and therefore, the potential for eavesdropping) varies with the technology used and the age of the screen. The technology for eavesdropping on electromagnetic radiation I will indicate with TEMPEST: Transient ElectroMagnetic Pulse Emanation Surveillance Technology. I derive this acronym from the standard which the US has developed for computer technology that is sufficiently shielded against electromagnetic eavesdropping. The standard was termed TEMPEST, an acronym⁷ for Transient ElectroMagnetic Pulse Emanation STandard. I will use the acronym in the broader sense to refer to the technology of eavesdropping; where I refer to the shielding standard, I shall term it the TEMPEST standard.

9.2.1. Description

Although TEMPEST has been around since the 1950s, the dangers of electromagnetic radiation became more widely known when Wim van Eck, a Dutch engineer working at the research laboratory of the Dutch PTT, published an article in 1985⁸ – which was immediately classified by the US government. Indeed, TEMPEST is clouded in secrecy, and the US makes a consistent effort to keep TEMPEST-related information secret. Enough information is extant, though, to get a picture of the possibilities of this technology.

Computer monitors (or Video Display Terminals) use an electron gun to fire electrons at the screen, which cause pixels to fluoresce. The electron beam scans across the entire screen many times per second. When the beam fires, it causes a high voltage emission of electromagnetic radiation (all electronic devices emit such radiation, but for the purposes of this chapter, reconstructing the contents of computers is by far the most interesting application). This electromagnetic radiation travels across considerable distances, and wires and cables may serve as an antenna, extending the emission range; also, power cables may serve as conducts of the emission. Now, with the proper devices and some technical knowledge, someone from a distance can pick up the radiation and, with synchronization, reproduce the original signal on a TV or computer screen. To get a clear signal, one may need sophisticated devices, but these are generally available – the sophistication required depends on the distance from which you pick up the radiation. Note, however, that modern computer screens

7 Or perhaps it is not – the US government denies it being an acronym, and says it was a code word without a particular meaning, according to [McNamara 98].

8 The article [Eck] was intentionally incomplete, as admitted in a sequel ‘Electromagnetic Eavesdropping Machines for Christmas?’ [*Computers & Security* No. 4 (1988)], but even so, others were able to replicate the results of van Eck’s experiments.

have generally much lower emission rates, and secret monitoring may therefore only be practical with somewhat older computer products.

Although laptop computers, which use a different screen technology, are better shielded from electromagnetic radiation eavesdropping (laptop LCD monitors emit less radiation than computer CRT monitors), it could be possible to eavesdrop on laptops as well: the fact that there are TEMPEST-certified laptops available indicates that there is a risk. [McNamara 98]

What is more, cables emit radiation as well. Peter Smulders, an Eindhoven University of Technology researcher, has experimented with eavesdropping on RS-232 cables (which, e.g., link computers with modems) and concluded that data “transmitted along an RS-232 cable connection may be vulnerable to interception at a distance. Eavesdropping experiments showed that RS-232 data signals can be intercepted several metres away from a target system, even when a shielded data cable is used. (...) [A]lthough the separation distance at which interception is possible is limited to several metres, in many circumstances eavesdropping can be done without attracting attention.” [Smulders] Like cables, power lines or metal (e.g., water) pipes can also transmit radiation. It seems, then, that with the proper technology (which Smulders claims to be relatively cheap), one can eavesdrop on what is transmitted between, say, a computer and a modem. Given the fact that many programs block passwords on the screen (typing stars instead of the password), eavesdropping on cables (which, of course, do transmit the password in the clear) is a valuable addition to the surveillance of monitors.

One (possibly biased and rather hollering) reporter recounts a TEMPEST expedition in Manhattan: “The World Trade Center was fertile. It afforded open parking areas nearby with millions of glass windows to snoop... we were most successful snooping the lower floors from the street. We borrowed a friend's office at mid-tower in the south building and were able to view CRT's [computer screens] in the north building easily. We headed east towards the New York Post newspaper offices and read the latest news off their monitors (which was printed the next day). We headed north towards City Hall and NYPD Police Headquarters. Guess what? They're not TEMPEST certified either... Neither is the United Nations” [and so on, Jones]. Although difficult to estimate the real value of this snooping enterprise, it does seem to indicate that very few companies and institutes have sufficiently protected themselves.

Indeed, equipment certified as conforming to the TEMPEST standard is expensive and can only be acquired with government approval. Apart from these TEMPEST-certified devices, there are ways to shield computers and peripherals yourself. The measures traditionally involve encapsulating the device or the room in enough metal to block radiation – building a Faraday cage around the computer or in the room will do the trick. Such measures are cumbersome and can be expensive, and one may assume only the paranoid will take the trouble to implement such measures. After all, a risk analysis will show there are other likely ways in which information may be gathered more easily than through TEMPEST monitoring. Recently, however, Markus Kuhn and Ross Anderson have proposed more cost-effective software solutions to shield against TEMPEST attacks; in particular, they propose a font which hardly reduces text quality for the user, but which filters out the text on a TEMPEST-eavesdropping monitor. [Kuhn]

9.2.2. Situations, crimes, and encryption

TEMPEST will be used to recover information that is processed on computers – stored files, e-mail messages, or web browsing. It may therefore be a good tool for the police to investigate organizational crime, which almost by definition makes plenty use of computers. The fact that most offices contain several computers is, surprisingly, not a drawback: TEMPEST monitoring easily distinguishes between computers; only when two computers consist of exactly the same components from the same manufacturers from the same batch, and no component has been updated in any way, will the radiation characteristics be similar [Seline], and this is rarely the case.

Likewise, it could be used to catch computer criminals ‘on the spot’, such as hackers or spreaders of illegal information, but as this requires suspecting someone in particular, this will mainly be effective for obtaining evidence, not for investigating a case. As to organized crime, it depends on the kind of criminal organization involved whether TEMPEST monitoring is an effective investigation measure – not all criminal groups use computers to communicate or to store incriminating information.

Since TEMPEST reproduces what the computer user sees on his screen, it will not be hampered by encryption: the user will type in plaintext before encrypting it, or will decrypt messages. To capture passwords (that protect encryption keys or access to the computer), in most cases, reproducing the screen will not help, since all except outdated operating systems shield ***** on the screen. Monitoring the cable will capture passwords or keys, but this generally requires a smaller distance – often, the adjoining room or, perhaps, building – and will therefore be somewhat less practicable. Monitoring screens can take place from a considerable distance, and may therefore be done from a mini van or from a building across the street.

9.2.3. Legal status in the Netherlands

TEMPEST has hardly been discussed in legal circles in the Netherlands; the only reference I know of is in the parliamentary documents of the Computer Crime Act. The Explanatory Memorandum states that the provision prohibiting the technical interception of digitally transmitted data (art. 139a DCC) also covers the interception of ‘residuous radiation’ emitted by computer devices [21551, nr 3, 17]. Therefore, TEMPEST monitoring is in principle punishable in the Netherlands.

To estimate whether the police could use it as an investigation measure, one must consider whether there is an analogous power that can be interpreted as including TEMPEST monitoring. Since it is a privacy-infringing measure, it requires explicit legislation; a potential power may not be interpreted extensively as including TEMPEST monitoring.

The potential analogous powers that come to mind are intercepting telecommunications (wiretapping), observation with technical means, ‘recording of places’, and direct eavesdropping. The power to *wiretap* can not include recording electromagnetic radiation, as the radiation is not transmitted across the public telecommunications infrastructure. *Observation with technical means* is a new power included in the draft law on special investigation powers; its goal is to observe persons or goods, and cameras or video recorders may be used. However, no communication may be recorded. As recording electromagnetic

radiation from a computer monitor will often involve communication, I would not interpret 'observation' as a power that includes TEMPEST monitoring.

The same goes for the '*recording of places*', a (new) power that aims at assessing whether a place contains illegal goods or traces; technical devices (say, cameras or video recorders) may be used for recording the traces, but no conversations may be recorded. Although one could suggest that TEMPEST monitoring is a way of securing traces (or to assess whether a place contains illegal information, such as child pornography), the casual nature of a 'peeping operation' is contrary to the systematic monitoring of a computer; moreover, the computer may also involve conversations or communications. Using the power of a peeping operation to record electromagnetic radiation would be *détournement de pouvoir*.

TEMPEST monitoring is most similar to *direct eavesdropping*, which is the recording of communications with technical means. The wording of the power was altered from 'conversations' to 'communications', in order to include a broader range of data traffic. Even if the law is interpreted as to include the recording of what someone is doing on a computer (see 9.1), the Explanatory Memorandum only mentions tape recorders, bugs, and directional microphones. Apparently, the Minister has not thought of recording electromagnetic radiation – TEMPEST is nowhere mentioned in the draft law on special investigation powers. Since investigation powers should be narrowly interpreted,⁹ the extension of direct eavesdropping to include TEMPEST monitoring is a step too far.

I conclude that the Dutch police is not allowed to use TEMPEST monitoring. Creating such a power is certainly possible, and given its similarity to direct eavesdropping, may also be considered realistic, or even desirable. It would help the police, as a useful supplement to using directional microphones. The indication that most computers are not shielded against TEMPEST monitoring suggests that the police could really benefit from such a power. On the other hand, it is one more power that severely infringes people's privacy, and one may well argue that the present range of investigation powers should be enough, the more so as the accumulation of various privacy-infringing measures can constitute an extra infringement.

9.2.4. Situation in other countries

Canada, in its Criminal Amendment Act of 1985, specifically included a reference to the use of electromagnetic devices to access computer data, which shows the intent to penalize the use of TEMPEST equipment. [Seline]

There are no countries that I know of that specifically authorize the police to use TEMPEST monitoring. Whether they are allowed by extensive interpretation of similar powers, depends on the national situation. In a case study with arguments pro and con the opinion that TEMPEST monitoring is illegal in the US (as an interception of an electronic communication, and/or as a violation of privacy by intrusion upon seclusion), Timothy Rabel quotes an interesting analogy: US police may use thermal imagers to detect temperature changes on the surface of objects (excessive heat from a building may indicate marijuana

9 Which is not to say that they always *are* narrowly interpreted. HR 8 November 1988, NJ 1989, 667 (search in rectum) interpreted the power to do a body search (literally: search 'on' the body) to include the power to do an internal investigation (search 'in' the body, in this case, the anus), which is a rather extensive interpretation.

cultivation). In *United States v. Penney-Feeney*, the “court held that the heat was not a protected communication but a byproduct or ‘heat waste’ in which the defendant could not expect privacy, similar to abandoned garbage and odors from a suitcase.” [Rabel] On the other hand, the Court of Appeals for the 9th Circuit ruled in *United States v. Kyllo* that an infrared scanner which records heat patterns is not merely recording ‘waste heat’, but may also offer information on intimate activities, and therefore violates the Fourth Amendment if used without a warrant. Although one could argue that electromagnetic radiation is a ‘byproduct’ or ‘data waste’ that does not warrant an expectation of privacy, the information leaked through data waste is more privacy-sensitive than heat waste information, and it seems likely that it is an infringement of privacy protected by the Fourth Amendment.

Although there are allegations that intelligence agencies have applied TEMPEST monitoring, I know of no cases of law-enforcement agencies recording electromagnetic radiation.

9.2.5. Conclusion

TEMPEST monitoring is an interesting option to retrieve data processed by computers. It is currently illegal for the police (at least, in the Netherlands), but the legislature could consider creating a power to this effect. One may be optimistic about the expected results of TEMPEST monitoring, although it would not be practicable in many cases: it can only target cases in which people use computers to process significant data, and it requires proximity to the premises. Still, the police could benefit from it as a supplement to data interception and direct eavesdropping. The fact that it is not hampered by cryptography and that it may sometimes yield encryption passwords or even keys makes it a valuable alternative. However, the infringement of privacy is considerable, and the legislature should conscientiously trade-off the expected benefits with the fact that it is one more power that many people would feel to be part of Big Brother’s Brave New World.

9.3. Infiltration

Technical measures, such as direct eavesdropping and TEMPEST monitoring, may yield valuable information, but they remain passive and are not very flexible to follow a criminal organization. In certain cases, it may be more effective for the police to simply approach the organization in person – undercover, needless to say. Through infiltrating a criminal organization, the police can see who is involved in what activities and, if they notice incriminating activities, can directly write their observations down in an official report. This yields another kind of information than wiretaps and computer searches, but it will be equally valuable for the prosecution.

9.3.1. Description

Infiltration is defined by the Dutch draft law on special investigation powers as “participating in or assisting a group of persons planning or committing crimes, under the direction of the public prosecutor for the sake of investigation” [25403, nr 3, 28]. It encompasses



many activities: long-term infiltration, pseudo-purchase (the 'buying' by the police of prohibited goods), pseudo-sale, operating a front-store (a fake company which offers services to criminals), controlled delivery (helping to deliver prohibited goods, in order to arrest the buyers and sellers on the spot), and 'con-trolled delivery' (allowing pro-hibited goods to be marketed). Infiltration can be done both by (undercover) police agents and by (law-abiding or criminal) civilians.

Infiltration, or more in general, undercover policing, is

an accepted practice in most Western countries, where it has been used at least since the early 19th century. In the Netherlands, chief inspector Waldeck may have been the first undercover agent, operating in the Hague around 1846; he gained the confidence of a gang of counterfeiters, and thus assured the arrest of the core culprits. [Frielink, 9] Towards the end of the century, the practice of *agents provocateurs* investigating – or rather provoking – alcohol crimes was heavily debated, until they were checked in 1889 by a circular from the Minister of Justice ruling that no investigating officer should provoke crimes. Undercover agents again gained public attention in the 1970s, when the increasing investigation of drug crimes provoked new means of investigation – the US Drugs Enforcement Administration (DEA) seems to have introduced the practice of infiltrating drug crime groups in the Netherlands. [Frielink, 19] Despite concerns over the lawfulness of the practice, it was institutionalized in the 1980s with training for infiltrators and the establishment of pseudo-purchase teams.

Practice has proven infiltration to be an effective tool in the investigation of organized crime (and, to a lesser extent, serious business and non-organized crime): it is “increasingly seen as an efficient and even necessary strategy to combat major crime problems” [Fijnaut, 1]. It has been used in all its manifestations by the Dutch police, notably long-term infiltration and pseudo-purchase [Traa, 232-274]. Indeed, the Dutch combination of public confidence in the police, lenient judges, and the generally accepted concern over serious organized crime seem to create “an optimal climate for covert policing.” [Klerks, 105]

Still, several risks are involved. As police chief Welten has put it: “As far as I am concerned, every infiltrator is definitely somewhat criminal. Perhaps you can be both reliable and criminal, but that is a contradiction which I can not really manage.” [quoted in Traa, 242] There is always a risk that the infiltrator is corrupted by the criminals whose company he is keeping, he may play a double role, or leak information to the criminals. He may even get so much used to the luxury of fast cars and fancy lifestyles, that after the termination of the infiltration, he ‘goes native’ and continues his criminal activities, this time not bothered by

supervision of the public prosecutor. Besides the risk of corruption, there is always the risk of the criminal organization exposing the undercover agent and retaliating upon him – or his family. Infiltrators thus have to steer between the Scylla of being credible to the criminals, which means committing crimes, and the Charybdis of being reliable to the police, which means keeping clean from unwarranted criminal activities – a hard task, for sure.

Then, there are practical difficulties. To diminish the risks for undercover agents, they should be specially trained police agents. The costs and time for training and for executing infiltration operations are significant. Also, there are organizations which no qualified police agent can enter because of cultural or language requirements, and some organizations are extremely closed to outsiders. In those cases, only a civilian close to the culture of the group could infiltrate. Apart from higher risks of corruption, civil infiltrators are less ‘steerable’ than police agents, and the judiciary cannot really control their criminal activities. Another problem is that civilians cannot write official reports (for court evidence in the Netherlands); they have to report to police officials, so that the incriminating reports are second-hand. In any case, the reliability of a civil infiltrator will be a prime target for the defense in court. A legal problem closely related to undercover investigation is the fact that in many cases, the undercover agent will want to remain anonymous (out of fear of retaliations, or because the police wants to remobilize him) – and the legal status of anonymous witnesses is still contentious.

9.3.2. Situations, crimes, and encryption

Obviously, one can only infiltrate groups, not single criminals. Therefore, infiltration is an investigation measure eminently targeted at organized crime. Its goal can be to delineate a criminal organization; it can also be used to gather evidence against specific suspects. It is in no way hampered by encryption, and, as such, it is a good alternative to wiretapping in the investigation of organized crime.¹⁰ To a lesser degree, it can replace or supplement evidence-gathering through searching computers – the evidence undercover agents can provide is generally quite different from evidence stored in a computer; in some cases, it may yield similar circumstantial evidence, but in most cases, the testimony of undercover agents cannot replace evidence of stored data. Still, evidence-gathering is also a valuable asset of infiltration.

Although undercover agents have the reputation to only infiltrate in criminal organizations, they are also deployed to investigate other crimes committed in groups. Thus, infiltration can be used in business crime cases, notably to investigate corruption and large-scale fraud; indeed, it has been used “against the most (...) unlikely of targets (...) to find corruption among police, prison officials, prosecutors, defense attorneys and even judges and legislators.” [Fijnaut, 24] The Dutch legislature also recognizes opportunities for infiltration in

10 Indeed, Simmelink argues for the similarity between wiretapping and infiltration: “The parallels between both investigation measures are the secret character of the state behavior and the breaking of the confidential character of the communication, enabled by a technical act (with telephone conversations) and by an investigation agent operating undercover (with infiltration). (...) The essence of both investigation measures is, after all, the same; in both cases, the state ‘eavesdrops’ in a devious and secret way.” [Simmelink, 46]

serious forms of non-organized crime (e.g., in murder cases), and for investigating certain forms of computer crime – for instance, online infiltrating a network of persons exchanging digital child pornography [25403, nr 3, 28-9]. In most of these cases, the infiltration can replace to a certain extent the gathering of information by wiretapping or by computer searches.

9.3.3. Legal status in the Netherlands

Infiltration has been allowed for a long time without an explicit legal basis. The practice of undercover agents in the 1970s was condoned by the courts; the landmark 1979 *Tallon* decision formulated the main requirement for undercover agents: they should not lead the suspect to other acts than he already intended to do. Besides this ‘Tallon criterion’, the principles of subsidiarity and proportionality also seemed to be requirements posed by the Supreme Court [Frielink, 27]. Following a study into opinions within the police and judiciary on the subject, the Minister of Justice released a report [19328, nr 1] in 1985 with conditions under which he considered infiltration acceptable. These were somewhat stricter than the case-law requirements, and included mandatory prior approval by the prosecutor and supervision by the chief detective. Also, the Minister preferred only specially trained police officials to be deployed. These constraints on infiltration were finally laid down in guidelines issued by the Public Prosecutor in 1991.

The practice of infiltration without an explicit legal basis has been contentious, because the investigation measure may infringe the constitutional right to privacy (and therefore would require an explicit legal basis), and also because the committing of crimes by undercover agents does not seem to be authorized outright by the legal grounds for exemption from criminal liability [Frielink, 35-72].

There is disagreement whether and to what extent infiltration infringes the privacy of people participating in a criminal organization. The European Court did not find a privacy infringement in the *Lüdi* case: “Mr Lüdi must therefore have been aware from then on that he was engaged in a criminal act (...) and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him.” Frielink argues that privacy is not at stake, mainly because infiltration involves purely business contacts [Frielink, 55]. In case of more structural infiltration, however, which usually involves activities far exceeding criminal business contacts, the privacy of suspects may very well be at stake. As the Dutch Minister of Justice states: “with infiltration, in certain circumstances, the privacy of the people involved can be at stake” [25403, nr 3, 30].

Following the recommendation of the Van Traa committee to create an explicit legal basis, the draft law on special investigation powers introduces specific powers for infiltration and pseudo-purchase. These are not only allowed for investigating specific crimes, but also for investigating organized crime more in general (in particular, to infiltrate a group which is suspected to scheme or commit crimes). Contrary to the Van Traa recommendation, the proposed law allows for civil infiltrators, if undercover police agents can not be appointed for the task. They sign a contract with the prosecutor regulating their rights (including an indication of the crimes they may commit) and duties. In extremely exceptional cases, even criminal civilians may be appointed to infiltrate (although they may not commit any crimes without prior written authority by the public prosecutor, a somewhat unrealistic demand).

Infiltration is allowed only for serious crimes (for which pre-trial detention is possible) which can pose a serious threat to the rule of law. The safeguards include the constraints posed by case law (including the Tallon criterion and the principle of subsidiarity), and pay attention to the control and supervision by the public prosecutor.

9.3.4. Situation in other countries

During the 19th century, infiltration became an accepted investigation measure in Western Europe. It was only gradually accepted in the United States, but in the course of the 20th century, it turned into a major investigation tool in the US – at the time when in Europe, it had become highly suspect after the experience with Soviet and Nazi covert policing. By the 1970s, the US practice gradually (re)influenced European practice, with the war on drugs and the advent of (political attention for) organized crime, and covert policing “again became routine European police activity” [Fijnaut, 15].

In most countries, there is a similar ‘Tallon’ requirement that the police may not provoke crimes, although its scope and the consequent proof issues differ per country [Frielink, 142-143]. In *Germany*, for instance, the case law on whether the undercover agent has ‘considerably influenced’ the suspect seems to indicate that undue influence is not easily assumed by the courts: there is considerable room for an infiltrator to ‘steer’ an action [Frielink, 117]. US courts judge whether the undercover agent has ‘entrapped’ the suspect, and they decide this mainly on the basis of the behavior and the past of the suspect (thus, for example, undercover agents can be more ‘provocative’ towards suspects with a criminal record than towards ‘unwary innocents’) [Frielink, 119].

The extent of infiltration also differs per country. In the *United States*, since the early 1980s, there have been about 400 FBI undercover investigations a year [Fijnaut, 13], whereas *Canada* has proportionally less undercover investigations – perhaps, as Brodeur notes, because Canada uses interception of communications about twenty times more, relative to the US, and because drug cases are much less important in Canada [Brodeur, 77-8].

9.3.5. Conclusion

Infiltration is an effective measure in the investigation of organized crime, as well as in certain other cases of crimes committed by groups, such as large-scale business crime, corruption, and online kid-porn exchange. Police undercover agents – or, in exceptional cases, civil infiltrators – can lay bare the structure of a criminal organization or gather evidence against the group committing or planning crimes. Infiltration does, however, involve high risks – both to the infiltrators (facing unmasking and retaliation) and to the rule of law (if the infiltrators are corrupted by the criminal environment and ‘go native’). Long-term infiltration also involves high costs for training police specialists.

To a considerable extent, infiltration is a viable alternative to wiretapping, untroubled by encryption. It will generally yield somewhat different information – the undercover agent will not observe all conversations, if only because he is physically bound to being in one location at a time. Still, he can provide information and evidence on the structure of the criminal organization, and in that respect, infiltration is a good alternative to wiretapping in the early stages of an investigation. However, it requires considerably more effort and time, and it

involves higher risks for the police. Therefore, infiltration can never replace wiretaps entirely. Although yielding different information than computer searches, infiltration is also important for evidence-gathering, and in that respect, it may fill some of the gaps in cases where encryption blocks computer searches and seizures.

9.4. Crown witnesses

*ROMAINE. But you do not understand at all. I knew he was guilty.
(Agatha Christie, The witness for the prosecution)*

9.4.1. Description

If the police does not succeed in pushing outsiders into a criminal organization, they may resort to pulling insiders out of the organization and have them testify against their (former) accomplices. As nothing works for nothing (especially with criminals), the police will have to offer the insiders considerable benefits: protection from retaliation and reduction of a sentence. Thus enters the crown witness: someone who in return for judicial advantages provides essential testimony against serious criminals.

Generally, the police finds evidence against many people participating in a criminal organization, but often, these are only lower people executing higher orders – the bosses remain conveniently veiled behind the curtains which no wiretap, directional microphone, or even undercover agent can readily draw. Crown witnesses know the core of the organization and can pinpoint the responsible top. They can therefore be a primary tool in prosecuting criminal organizations, and especially the top thereof.

Whereas a crown witness is generally associated with criminal organizations, he may also feature in certain business crime cases, notably in major fraud schemes of otherwise (supposedly) respectable enterprises. The evidence provided is of a different kind, however, than books or computer files that show direct evidence of a fraud. In the general business crime case, the police may not have to use the commercial crown witnesses as a last resort because other investigation measures can provide sufficient evidence. Only with the most serious cases of business crime would the crown witness be an option; in those cases, one can probably speak of the business as a criminal organization as such. Therefore, in this chapter, I will treat the crown witness as a character in organized crime cases only.

What makes this measure extra appealing is the fact that, contrary to most investigation measures, criminal organizations can hardly take counter-measures: they can only prevent people from defecting through severe intimidation. The police can parry this intimidation with a trustworthy, effective protection scheme. To be sure, the success of having crown witnesses relies on the efficacy and reliability of this protection program. Since the witness has defected from a criminal organization to the police, the organization will try its utmost to retaliate: silence the witness, preferably through killing him, or else through killing his kin or dear.¹¹ Therefore, the state must not only protect the witness, but also his (close) relatives,

¹¹ The reaction of the Italian mafia to the first *pentiti* ('penitents') was to try to kill them. Then, they tried to discredit the *pentiti* system by 'infiltrating' with false penitents. When this did not work, the mafia resorted again to killing the penitents. [Manunza 94, 64]

for a long time. (In areas where family ties are very close, such as Calabria in Southern Italy, a protection program may involve over a hundred family members!) In most cases, this will mean that the witness and his or her close relatives will move to another (part of the) country and assume a new identity. (The Netherlands being the small country that it is, real protection can only be sought abroad.) The costs of such a program are therefore considerable – not only financially, but also psychologically. It is clear that states can only afford a limited number of crown witnesses, if they can attract them at all. (Note that with criminal business organizations, the use of violence against traitors may be less natural, and so, a witness protection scheme may be less necessary.)

Although several countries stage crown witnesses in criminal proceedings, typically in organized crime cases, the character remains controversial. After all, although a crown witness can provide evidence and insights into a criminal organization which no other investigation measure can match, who is to say that he – a criminal, for sure – speaks the truth? And does not the fact of reducing punishment for some criminals undermine the very essence of criminal justice – punish the same crimes with the same punishments, and punish according to the amount of guilt?

Many of the drawbacks and doubts can be addressed in a careful statutory regulation of the way in which crown witnesses may be staged in criminal cases [Asbeck]. The disputed reliability of crown witness testimonies is not a serious problem. Judges will view their statements with extra caution (judges always assess witness reliability, and they will naturally be more wary with crown witnesses), and they will check their information with other evidence (a conviction should never be based on crown witness evidence alone). Thus, in Italy, the law demands independent supporting evidence for crown witness statements. More importantly, crown witnesses have every reason to cooperate: if their statements are found to be false, their sentence reduction will be reviewed, and they may also be prosecuted for perjury or calumny. Moreover, government protection will stop, and they will be at the mercy of the criminal organization they defected – in many cases, this means certain death. Experience in Italy shows that legislation and case-law have developed an adequate set of guarantees for the reliability of crown witnesses [Manunza 98].

However, there are more fundamental arguments against crown witnesses. The state protection program can turn against itself if the crown witness commits new crimes with the help of his new identity (see [Abadinsky, 490] for examples of such wayward witnesses). Also, it seems contrary to the (Dutch) criminal system to bargain with criminals about punishments, although, in practice, this is happening frequently in, generally, less grave cases. A more fundamental argument is the fact that punishment should be related to the amount of guilt of the perpetrator – reducing punishment for reasons that have nothing to do with the crime in itself is detrimental to the credibility of the legal system. Although these objections can be met to a reasonable extent by having a judge evaluate the deal in court according to clearly established criteria (subsidiarity and proportionality for one), which makes the procedure controllable and transparent, there will always remain an amount of inequality before the law: similar crimes may be punished differently according to a perpetrator's accidental testimony in another case. This is inherent to any regulation involving crown witnesses, and must be accepted if the benefits are considered to be significant enough for the prosecution of organized crime.

9.4.2. Situations, crimes, and encryption

Although someone suspected of a crime may in principle know something about any other crime or criminal, most people consider a crown witness to be someone testifying against an organization in which he himself participated – it will therefore concern organized crime. Given the fact that allowing crown witnesses potentially undermines the credibility of the entire criminal procedure, it will only be allowed in serious organized crime cases, and then only as a last resort. The judiciary can only consider adopting a crown witness, if there are no other ways left to investigate and prosecute a criminal organization.

Crown witnesses appeared on the criminal stage in several countries in the 1970s, mainly in terrorism cases – in Germany and Italy, they were found to be virtually the only way to penetrate closed extremist groups. Later, they were used also in kidnaping and drug cases, and in other forms of serious, organized crime. In Italy, crown witnesses (called ‘cooperators with the judiciary’) are now mainly used in mafia cases. In the United States, the witness protection program is used in cases involving organized crime, drug trafficking, other serious federal felonies, state offenses similar to the federal categories, and certain civil and administrative proceedings in which a testimony may jeopardize a witness [Shur, 67]. In Belgium, Denmark, and Germany, the crown witness plays a part in drug trafficking cases. [Tak 94b, 147]

Evidently, encryption does not hamper crown witnesses. On the contrary, it is a valuable tool in the protection program, which often involves complex procedures for letting the witness-with-a-new-identity communicate with the beloved ones of his former life.

9.4.3. Legal status in the Netherlands

In 1983, the Ministry of Justice issued guidelines for deals with criminals. These involved procedures and guidelines for the prosecutor to ‘bargain’ with criminals, but they did not touch upon crown witnesses. A witness protection program was introduced in 1993, which can be used in organized crime cases and matters of life and death; in exceptional cases, a change of identity can be part of the program. Case law has accepted a crown witness in a few cases,¹² although opinions differ on the extent to which these decisions okay crown

12 The most important case is Hof Amsterdam, 30 January 1998, in which key statements by crown witnesses Karman and Abbas were used to convict Johan V. ‘the Stammerer’. The Court considered the statements reliable, in particular because they were detailed and consistent, supported by other evidence, and because the defense had had ample opportunity of examining the witnesses. The Court did, however, lower the sentence of ‘the Stammerer’, because the Public Prosecutor was not authorized to promise Karman that if he were convicted, they would not execute his sentence. Other cases that involved statements by people who had been promised judiciary advantages were so ‘a-typical’ that the term crown witness is perhaps not justified. [HR 15 February 1994 and HR 19 March 1996, *NJ* 1997, 59]

witnesses in general. The Van Traa committee counseled against immunity for crown witnesses, mainly because they thought it too grave a measure, given the fact that organized crime does not threaten democratic institutions in the Netherlands. However, the Public Prosecutor updated the guidelines on bargains with criminals in early 1997 to include crown witnesses: under the conditions of proportionality, subsidiarity, openness, and review during trial, the prosecutor can promise the testifying criminal to demand a lower punishment against him or to alleviate the execution of his punishment. Such bargains require prior evaluation by the top of the Public Prosecutor.

The Minister of Justice agreed that crown witnesses are a valuable investigation measure, and started drafting legislation in 1997. After considerable reflection, a legislation proposal was approved by the Council of Ministers in April 1998 and sent to the Council of State for advice. By July 1998, it had not yet been submitted to parliament. The draft law allows – with extreme reticence – ‘pledges to criminals’ in very serious cases, punishable with at least eight years’ imprisonment. The conditions are similar to those of the Public Prosecutor’s guidelines. The pledge is subject to review by an examining judge, and a court can only reward the crown witness for his cooperation by reducing his prison sentence by at most a third, or by replacing part of the prison sentence by a fine. Moreover, the law stipulates that no-one can be convicted on the basis of crown witness statements alone.

9.4.4. Situation in other countries

The *United States*’ Federal Witness Protection Program, meant for criminal insiders who are at risk because they cooperate with law enforcement to provide evidence against other criminals, has been effective since the 1970s in combating organized crime. According to one of its directors, “without the Program the convictions of tens of thousands of high-ranking members of major organized crime groups throughout the United States could not have been obtained.” [Shur, 69] Between the early 1970s and 1994, over 6,300 witnesses and over 7,950 family members were taken up in the protection program. *Canada* made extensive use of crown witnesses (‘delators’) between 1972 and 1986, but the testimony of one delator that the police had incited him to present false evidence led the Supreme Court in 1988 to imply that “the use of paid delators tended to bring the administration of justice into disrepute” [Broudeur, 80].

In *Italy*, reward regulations were introduced in the late 1970s and early 1980s for collaborators with the judiciary in terrorism and kidnap cases. The regulations were extended in the early 1990s to cover drugs and mafia cases as well. At the same, a witness protection program similar to that in the US was introduced. By March 1994, 668 witnesses and some 3,000 to 4,000 family members had been taken up in protection programs. [Manunza 94, 53] It is considered an essential, effective, and reliable tool in combating various forms of organized crime and, in particular, the mafia. In *Germany*, in the early 1980s, a crown witness regulation was introduced for drug trafficking cases, which allows the judge to decrease punishment of a member of a criminal organization who provides information on drug crimes; the suspect need not necessarily testify in court, and so he need not be a ‘crown witness’ proper. The regulation was used over 500 times in the first year and a half of its existence. [Tak 94b, 66] It was followed by a 1989 crown witness law for terrorism cases, in which a crown witness can be indemnified from prosecution or given a lower punishment.

The law contributed to gaining insight in the organization and strategies of terrorist groups, and confirmed the correctness of earlier convictions of RAF terrorists. Although the law was at first heavily debated, notably because it is contrary to the German principle of legality which requires the prosecutor to prosecute all crimes, the debate has cooled down since its establishment. [Tak 94b, 148]

9.4.5. Conclusion

Crown witnesses can be valuable in prosecuting organized crime, as they give essential insight into the core and top of criminal organizations; they may also sometimes be useful in the most serious cases of business crime. They provide to some extent an alternative to wiretaps, and less so to computer searches (the information turnout is comparable to infiltration in this respect). Although their statements must be viewed with caution, there are enough guarantees that crown witnesses provide reliable statements – it is in their own interest. Since the system of crown witnesses may undermine the essence of criminal justice (punishing crimes in proportion to people's guilt), it is a legally controversial measure. This, together with the practical problems and high costs involved, means that crown witnesses may only be staged in a very limited number of cases. Whether a state allows crown witnesses at all is a matter of criminal politics: balancing the benefits of combating organized crime in a way unparalleled by other investigation measures with the drawbacks of a potentially less credible criminal justice system and the costs involved. Several countries, notably the US and Italy, have decided in favor of the crown witness, and their experience so far seems to be favorable within the context of their legal systems. A Dutch draft law would also, under strict conditions, clear the way for crown witnesses.

9.5. Data mining

Of course! How could Carol have known Alice was reading 'The witness for the prosecution' if she hadn't spoken with her in two weeks? It must have been her who killed Alice... In the last pages of whodunits, the detective often puts together several separate information pieces (carefully hidden by the novelist) to deduce who did it. The answer was there all along, only you did not see it earlier. Combining data can give you new information, and this is the essential principle of 'data mining'. If the police fails to retrieve new pieces of data, they can resort to smart techniques to re-examine the data they have – and the police have loads of data: much more than they have information. Data warehousing and data mining can be useful tools for the police to supplement their news-gathering activities. It is not a genuine investigation measure, but more an information management tool. In that respect, it can hardly be considered an 'alternative investigation measure'. I will discuss it nonetheless, since a better information management may also serve to improve the information-gathering results by the police in general.

9.5.1. Description

Data mining is a relatively new technology used mainly by enterprises for marketing purposes. Over the past few years, *data warehousing* has risen as a necessary first step for the data mining process. This refers to building (ultra)large data bases in such a way that they can be searched by more or less intelligent tools. A data warehouse (often built up of smaller 'data marts') is a collection of basic data, such as personal data, postal code data, telephone traffic data, and buyer and seller data. *Data mining* is the technique to retrieve information from such data bases – not the basic information, but 'added-value' information. Until recently, only more or less trivial queries were used to retrieve information from data bases. Nowadays, smarter technologies, such as neural networks, visualization techniques, and genetic algorithms, are emerging, which search in a more intelligent way. The entire process is best referred to as 'knowledge discovery in data bases' (KDD): "the non-trivial extraction of implicit, previously unknown and potentially useful knowledge from data" [Adriaans, 5].

The process of KDD typically involves the following steps: building a (large) data base, selecting data to search, cleaning, enriching, coding, mining, and reporting. That is, about 80 per cent of KDD concerns preparing the data. Cleaning is important, because often, a significant percentage of data in a data base is polluted (double entries, outdated data) – and the basic rule in KDD is 'garbage in, garbage out'. After cleaning, the data can be enriched by adding new data, such as the average house price per postal code or car registry data. Coding (redefining data into mutually comparable digital data) is necessary to enable efficient searches. The mining process will then yield new data, which can be evaluated and used. The entire process is often recursive, and several steps will interact.

9.5.2. Situations, crimes, and encryption

There are a lot of data around, in uncountable data bases. For the police, several data bases are interesting to explore for data mining purposes: police registries, intelligence registries, municipal, social security, and car license registries, public data bases (such as Chamber of Commerce or land register data), private-enterprise data bases (such as subscription data or buyer information), and commercial data bases (marketing data, user or buyer profiles), et cetera. Of course, not all of these data bases can be accessed or used forthwith for law-enforcement purposes, but in principle, data marts that can be used for building a law-enforcement data warehouse abound.

What is more, the police can gather new data themselves to build the data warehouse. For instance, the police can collect telecommunication traffic data for a certain period on a (large?) number of telephone connections, or they can scan the air to record pager traffic data, or perhaps they can scan Internet connections for e-mail messages containing certain words or codes. (See 9.5.3 for a discussion whether this is legally acceptable.) In Germany, for instance, the intelligence service (*Bundesnachrichtendienst*) regularly scans the international telecommunications transmitted over the air on key words to pick out 'suspect' messages (this is called electronic *Rasterfahndung*). [Pfeiffer]

After collecting several data sources, data mining can help the police in two ways. First, mining a warehouse may yield interesting patterns or profiles, e.g., of people convicted for drug dealing or murder. Second, such profiles may be used for tracing suspects. The German intelligence service has apparently combined air flight data with holiday house renting data, since terrorists were found to be avid flyers and to rent holiday houses in winter. Persons who matched both properties were consequently good targets for further investigation. Such

profiling and matching techniques have also been used lately by Dutch IRTs to conduct 'phenomenon investigation', that is, screening certain sectors of society on their criminal behavior or, conversely, examining criminal processes on general characteristics. Once 'phenomenon investigation' yields profiles of suspect behavior, data bases can be mined to match persons or organizations.

Such profiling and matching techniques will yield a certain number of potential suspects – one should always bear in mind that matching a profile can never be equated with possible criminal behavior (a German scholar may well like to fly to quiet Pacific islands in summer and spend his winters on the Lueneburger Heide in order to write scholarly books). These techniques therefore do not constitute investigation; rather, they can be indicated as 'prevestigation' – the stage preceding actual investigation of a crime or criminal group. Prevestigative profiling and matching can be useful in examining individual or organizational fraud, or for examining criminal group structures. It can yield persons who merit further study or keeping an eye on.

The second use for the police is in the stage of investigation proper. The converse use of profiling and matching is to start with someone suspected of certain criminal behavior, and to use KDD to see whether he matches a profile associated with such behavior. If he does, this will serve to reinforce the suspicion – it could even be used (with proper reserve) as supporting evidence. Also, the combination of a concrete suspicion with additional data gathered, such as telephone traffic data, can lay bare possible group structures. Finally, the police can match data bases with personal data that match specific characteristics of the suspect. For instance, one can compare a data base with all owners of a red Volkswagen in Hamburg with a list of Hamburg customers who have payed their electricity bills in cash (as terrorists seem wont to do). Germany has a specific investigation power that regulates such automatic comparing of data bases for investigation purposes (called *Rasterfahndung*).

9.5.3. Legal status in the Netherlands

'Phenomenon investigation' may use KDD to screen a sector of society on suspicious behavior, but the use is limited through data protection laws. Both the Dutch Police Registries Act and the Dutch Data Registries Act (and the future Data Protection Act) apply to using and merging data bases for law-enforcement purposes. Although not all data bases contain personal data, many of the data somehow relate to persons (e.g., through address information or telephone numbers), and especially the merging of distinct data bases may create personal data if they do not already contain them. If the goal of the data mining process is profiling (which is the case, e.g., in 'phenomenon investigation'), the data can be anonymized (or, if desirable, pseudonymized through encryption, cf. 3.2.3) to avoid data protection obstacles. If the goal, however, is to match a profile with a data base to find (potential) suspects, anonymizing can not be used; in these cases, the goal-binding principle of data protection law will generally prohibit data mining, as most data bases are not built for such purposes. On the other hand, law-enforcement agencies may create data bases themselves, e.g., of telephone traffic data or pager scans, but in that case, the recording of such data must be compatible with criminal procedure law, and the police will require approval by the public prosecutor or the examining judge to gather such data.

In the meantime, the Ministry of Justice has discovered the potential of data mining. In its policy document *Legislation for the electronic highway* of February 1998, it proposes

research on data mining as an investigation measure. It would be allowed only in case someone is suspected, during an exploratory investigation, or in the investigation of organized crime where there is not a concrete suspicion. The trade-off with privacy must carefully be addressed, and the law should at all times specify whether the police can do occasional searches on a person, or whether they can use data mining at large. [25880, nrs 1-2, 197]

9.5.4. Conclusion

In all, KDD may be an effective tool for law enforcement: in preinvestigation to yield material to start a criminal investigation, and in the early stages of criminal investigation to lay bare potential criminal structures, and to match suspects with known criminal profiles. Data mining is generally allowed as far as it is targeted at profiling, and provided data protection law is taken into account. If it is targeted at matching and finding potential suspects or supporting evidence for known suspects, data mining may only use data bases created for the purpose.

Evidently, data mining will never be a major tool in itself, as it must be used in conjunction with other information-gathering techniques. In this sense, it can never replace wiretaps or searches, and as such, it is not a proper alternative if these measures are rendered powerless through encryption. It may be a supplementary tool, however, to compensate for the loss of new information as wiretaps and searches yield less and less information through increasing encryption use. Obviously, KDD itself is never hampered by encryption, as it uses plain data.

9.6. Assessing the alternative investigation measures

9.6.1. The options of alternative investigation measures

Looking at the five investigation measures outlined in this chapter, what are the options relevant to the crypto problem? First, one must distinguish between, on the one hand, investigation measures that are already allowed or will most likely be allowed in the near future (direct eavesdropping and infiltration), and, on the other hand, measures that are currently or may shortly be allowed in only a limited number of cases (crown witnesses and data mining) and measures which are not allowed at all (TEMPEST monitoring). Policy options of course can only address the latter: allowing new measures or significantly widening the application of restricted measures. Thus, only TEMPEST monitoring, crown witnesses, and data mining would be considered options. The other measures (direct eavesdropping and infiltration) should rather be taken as part of the context in addressing the crypto problem.

Second, one must distinguish between measures that are more or less natural alternatives to wiretapping and computer searches (direct eavesdropping and TEMPEST monitoring), and measures which are far removed from the traditional measures hampered by cryptocriminals. In this sense, only direct eavesdropping and TEMPEST monitoring can be considered 'options' to address the crypto problem; the other measures hardly relate to the crypto problem at all. Cryptocriminals are only one of the arguments in the broader debate over

infiltration, crown witnesses, and data mining. If such powers are enacted for other reasons than cryptocriminals, they may have the side effect of making the crypto problems for law enforcement less acute, but this will never be their main purpose.

Combining these distinctions, only TEMPEST monitoring would emerge as an option to address the crypto problem. However, I think that other – relatively minor – partial options also merit being taken into account. With direct eavesdropping, assuming that the current law proposal is enacted, one can consider lowering the conditions for eavesdropping within homes. With infiltration, one cannot, I think, lower the conditions for allowing it (it can by definition only be used in serious organized crime cases). It might be considered an option, however, to extend its scope and to use it in more cases (in other words, the option is to apply the principle of subsidiarity less strictly in applications for an infiltration warrant). Likewise, one may consider allowing crown witnesses in more cases than only the exceptional cases for which they are now envisaged. Data mining, however, remains too far removed from the crypto problem to consider it an option for the purposes of this book. It is an interesting tool for the police to research, and if it is employed, it must be taken into account when judging the overall potential of the police to gather information.

Thus, I arrive at the following options.

Option 9.1 Allow (more) direct eavesdropping, in particular within homes

(I assume here that the draft law on special investigation powers will be enacted; thus, the police has the power to eavesdrop directly, and they can use this power within homes only in cases involving crimes punishable with at least eight years.) The legislature lowers the conditions for allowing direct eavesdropping within homes, for instance, to crimes for which pre-trial detention is allowed (roughly, crimes punishable with at least four years). The legislature can also consider allowing direct eavesdropping for non-communications, i.e., for non-networked computers, talking in oneself, and the like.

Option 9.2 Allow TEMPEST monitoring

The legislature creates the power for the police to eavesdrop on electromagnetic radiation emanating from computers, under conditions similar to those for direct eavesdropping.

Option 9.3 Allow infiltration in more cases

The courts are more lenient in granting permission to infiltrate. The government provides extra money for training and protection programs for undercover agents. The legislature can consider dropping the subsidiarity condition for civil infiltrators (according to the draft law on special investigation powers, a court can only give permission for a civil infiltrator if it is not possible to employ a police infiltrator).

Option 9.4 Allow crown witnesses

If the law proposal on pledges to criminal witnesses is enacted, the legislature lowers the conditions for staging a crown witness (i.e., allows it in more than only the most serious and exceptional cases). Or, if the proposal is not enacted, the legislature reconsiders enacting it in light of the crypto problem.

9.6.2. Applying the criteria

1a. Privacy and the right to confidential communications

Options 9.1 and 9.2 substantially infringe privacy. Especially if the powers are allowed to eavesdrop within homes, the privacy infringement is severe – perhaps more severe than the privacy infringement of wiretaps. After all, people know that what they say over the phone can in principle be overheard (if only because one occasionally encounters others on the line). Currently, people have a complete expectation of privacy on what they say within their home (which is precisely why the Dutch Minister of Justice at first did not want to allow direct eavesdropping within homes). Moreover, it is not only what people say in their house, but also what they do that can be overheard: what music they listen to, when and how long they take a bath, and perhaps even what they write in their electronic laptop diary. TEMPEST monitoring can only intercept computer activities, and as such is less privacy-infringing overall; on the other hand, some computer activities may be more privacy-sensitive, such as writing personal letters, or surfing the Internet.

One can argue that the chance that a law-abiding citizen is the victim of a direct eavesdropping operation is small, and so, the expectation of privacy within the home would not be significantly altered by granting the police this power. After all, a similar development has taken place with the phone: people at first were cautious in trusting its confidentiality, whereas nowadays, most people are not particularly worried that their phone conversations can be overheard, particularly since the (Dutch) police is not known to do extensive (illegal) wiretapping. With direct eavesdropping and TEMPEST monitoring, public feeling may go the same way. On the other hand, one can also argue that the powers of direct eavesdropping and TEMPEST monitoring are perceived as more threatening powers, perhaps because they are closer and more direct – think of the specter Orwell has raised by putting two-way screens in 1984's homes. Especially in countries where the government has shown itself not to be very particular about citizens' rights, such powers are extremely threatening. My feeling is that direct eavesdropping and TEMPEST monitoring are significantly privacy-threatening (even in the Netherlands where people generally trust the government), in particular in view of the rapid development of surveillance technologies.

Infiltration is much less privacy-threatening. In some cases, law-abiding citizens may meet undercover agents under sensitive circumstances, but the chance that this infringes their privacy is remote (much more so than with direct eavesdropping). With crown witnesses, privacy is not at stake.

1b. The right to a fair trial

Provided that the evidential value is safeguarded (legislation or regulations should define standards of care for the gathering of evidence) and carefully assessed in court, none of the optional measures need infringe the right to a fair trial. With infiltration, one could argue that the testimony of an undercover agent may not always be refutable; the defense may be at a disadvantage to challenge the reliability of the evidence. The same goes, in principle, for crown witnesses. This concern can be addressed by the judge in paying particular attention to assess the reliability of the undercover agent or crown witness. Still, using evidence from undercover agents or crown witnesses may be somewhat detrimental to the rights of the defense if they have insufficient opportunity to question the witness themselves.

1c. The rule of law

As to *effectiveness*, all measures hold promise. Direct eavesdropping, especially bugging, is an effective investigation measure that can to a certain extent replace wiretaps. It is not usable in all cases, since it is confined to a specific location and it involves a risk of discovery; therefore, it cannot be used in quite as many cases as wiretaps. TEMPEST monitoring can yield the same kind of information as wiretaps or, to some extent, computer searches, but it can be used in far less cases, since it requires close proximity; moreover, there are rather strong technical limits to what can be retrieved with this measure. Infiltration and crown witnesses are also effective investigation measures, perhaps more so than direct eavesdropping, but their use is restricted to the more (or most) serious cases of organized crime. As alternatives to wiretaps and computer searches, they cannot really be considered effective as such, since they yield quite different information and are limited to organized crime (and the most serious cases of business crime) only. As options to address the crypto problem, then, their effectiveness is limited.

The *rule of law in general* is at stake because the first three options are extensions of intrusive observation powers. If enacted with the proper checks and balances, such powers need not infringe the rule of law – in the Netherlands, I expect that such powers would not be abused by law enforcement, at least not to the extent that the rule of law is threatened. (In countries with a less supervised role for government, one must consider whether allowing such powers does not give a blank check for government surveillance.) Infiltration may be somewhat more threatening to the rule of law than direct eavesdropping or TEMPEST monitoring, since it involves a risk of corruption. As to crown witnesses, this measure does infringe the rule of law considerably: it negates the principle of punishing according to guilt and of punishing similar cases in similar ways, and it allows criminals to get away with a minor punishment.

1d. The right to economic development

The right to economic development is not at stake, since all options leave crypto use unharmed.

2a. A solution must be workable

The technology for direct eavesdropping and TEMPEST monitoring is available, but it has its limits in practice – directional microphones may not work if there is a lot of background noise, and TEMPEST monitoring requires close proximity; bugs are good enough, but they require breaking into places and may be discovered. Thus, these options can be implemented, but only to a certain extent. The same holds for crown witnesses: they can be staged only if there is someone available within the criminal organization and if there is a reliable protection program. Infiltration seems the best implementable, although it requires considerable costs.

None of the options are without risk of abuse. Bugs and directional microphones may be employed without a warrant, an undercover agent may go native, a crown witness may not keep his part of the bargain (for instance, by not telling the whole truth). The courts will supervise this, but their enforcement of the powers may leave gaps for abuse. At least, the measures at stake are less enforceable than wiretaps or computer searches, since these require

the cooperation of third parties (telecom operators and house owners) who can also see to it that the power is used according to the law. Therefore, the enforceability of the options is not optimal.

2b. A solution must be internationally compatible

Investigation measures are rooted in national investigation culture, and so, these options can well be implemented on a national scale, regardless of what other countries do. Only with infiltration, there might be a problem if in the investigation of an international criminal organization, an undercover agent gathers evidence against citizens of countries in which infiltration is not allowed. Since most countries allow infiltration, this need not be a significant problem.

2c. A solution must be technologically sustainable

Direct eavesdropping is defined in a functional, technology-neutral way, and thus is technologically sustainable. TEMPEST monitoring is more dependent on state-of-the-art technology, and developments in computer screen and peripherals technology may significantly limit the viability of this measure; it does therefore not seem very sustainable. Infiltration and crown witnesses, of course, are eminently sustainable from a technological point of view.

Figure 9.1 gives a simplified illustration of how the options match the principles.

<i>principles</i>	<i>options</i> direct eavesdropping	tempest	more infiltration	crown witnesses
1a privacy	–	–	+	+
1b fair trial	+	+	±	±
1c rule of law -effectiveness	±	±–	±–	±–
-general	±+	±+	±	–
1d economic development	+	+	+	+
2a workable	±	±	+ / ±	±
2b international	+	+	+ / ±	+
2c technology- neutral	+	±–	+	+
<i>overall estimate</i>	±–	–	±	±–

Table 9.1. Alternative investigation measures and options

– infringes principle

± has mixed effects on principle, infringes to a smaller extent

+ does not infringe principle

9.6.3. Conclusion

Various investigation measures, unhampered by encryption, can to a certain extent replace or supplement wiretapping and computer searches. Direct eavesdropping, especially bugging, is a natural alternative to wiretapping, which can record plaintext conversations. Likewise, TEMPEST monitoring may reproduce a computer screen, and thus reveal information someone is sending or storing before encryption (or after decryption); it may also retrieve passwords which protect cryptographic keys. Both measures have practical shortcomings, however, and, more importantly, pose a severe threat to people's privacy.

Infiltration and crown witnesses may be employed to gather first-hand information from within a criminal organization, and as such, are well tailored to laying bare the structure of a criminal organization and to gather incriminating evidence. Thus, they are alternative information sources to wiretaps and computer searches in organized crime cases. Both infiltration and crown witnesses involve high personal risks, and they may undermine the credibility of the rule of law. They can therefore be used only sparingly.

Data mining for profiling and matching criminal behavior is not a proper alternative to wiretapping or computer searches, and thus not an option.

All measures more or less infringe constitutional rights or undermine the system of law itself; only the option of extending infiltration need not seriously infringe the constitutional rights involved. Moreover, their effectiveness to fill the information gap caused by crypto-criminals is limited. So, there must be strong arguments in favor of them to balance their negative implications, if one is to choose one of these options to address the crypto problem.

Since these measures are part of a larger debate on investigation measures, one can hardly argue pro or con only on the basis of the crypto debate. There may be other compelling arguments for allowing direct eavesdropping in homes, for infiltrating more, or for staging crown witnesses. In the context of this book, however, I cannot take into account the broad issues involved in discussing these investigation powers. I will therefore abstract from the general debate, and argue whether one or more options should be considered only on the basis of the crypto problem, disregarding other reasons for choosing (or rejecting) them. This may be artificial for the legislature, but it is helpful for the argument in this book – it is the only way to compare this direction with the other optional directions.

Whether the fact that encryption increasingly hampers wiretapping and computer searches is strong enough to choose one of the options (and thus, to infringe constitutional rights) depends on several factors, notably the number and kind of cases in which the police uses or is dependent on wiretaps or computer searches, the extent to which uncrackable encryption is encountered in such cases, and, not the least, the national investigation culture and the nature of constitutional protection in a country. One must also take into account the effect of the *combination* of new investigation powers, which can pose additional threats to constitutional rights, in particular to privacy. Implementing several new powers that each help to partly diminish the crypto problem for the police could well lead us one step forward and three steps backwards, into the world of 1984. Privacy is not a salami to be continually sliced down. Whether the crypto problem is big enough to cut another slice of more investigation powers, can only be determined in an integrated analysis of the crypto dilemma, including the other optional directions, which I will attempt in Chapter 11. But first, I will discuss a final option: deciding not to choose one of the options discussed so far.