

## Chapter 10. The zero option

Doing nothing is often doing something. The effects of failing to act can be just as serious as the effects of acting. In some cases, the effects of neglect are even considered grave enough to be punishable, e.g., not filling in your tax returns form, or not throwing the lifebelt you are standing next to when someone shouts to you “Help! I can’t swim!” while slowly submerging. The same holds for the government: some situations call for action, and if the government fails to act, it is seriously remiss. On the other hand, a failure to act can sometimes also be a conscious decision, for instance, because the time is not yet ripe for action, or because one expects the problem to solve itself.

In the crypto case, the situation calls for action: cryptography is spreading rapidly, and ever more criminals will use it in the near future, so that criminal investigation will be seriously hampered. However, inaction is an option to take into account as well, given that the options to (actively) address the problem all have their flaws. It is at the extreme end of the spectrum of ‘solutions’, which has at its other extreme the banning of cryptography (Chapter 6½). In a way, it mirrors a crypto ban, with by and large reverse effects for society as a whole, i.e., the loss for law enforcement is significant, but the benefits for the information society at large are also significant. Therefore, inaction *is* an option to consider.

### 10.1. The zero option

#### *Option 10. Decide to do nothing*

The government decides not to take specific measures to regulate cryptography and not to take additional measures aimed at securing future information-gathering powers specifically to redress the decreasing effectivity of wiretaps and computer searches caused by crypto use.

One of the advantages of this zero option is that it is clearly feasible and technology-neutral – one need not analyze the *how* of this option. It is the *effects* that matter in assessing its desirability.

What are the consequences of doing nothing for law enforcement? If the government refrains from taking measures to ensure the future effectiveness of wiretaps and computer searches (or to establish alternative measures instead), the continuing spread of cryptography will inexorably hamper investigation (compare Chapter 4). Regardless of whether the government stimulates crypto use (for instance, through establishing a national public-key infrastructure), cryptography will soon be widespread and used by the vast majority of information society citizens. It will be built-in in major computer e-mail programs, web browsers, and operating systems, ensuring that virtually all electronic communications will be encrypted in the near to middle future. However, telecom providers are obliged to provide

for tappability, and so, the building in of cryptography in the information infrastructure need not hamper law enforcement. Crypto phones and crypto facsimile machines will become more widely available, although not necessarily everyone will use one (criminals, for that matter, will not hesitate to buy them). The market will provide standards for all kinds of crypto products, just like PGP became a de facto standard for private e-mail encryption in the middle 1990s. As the US National Research Council concluded in 1996: “the widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run.” [NRC, 300]

For wiretaps, this development would mean that the police will not be able to get at the content of all electronic communications. The effectiveness of voice wiretaps will slowly but surely decrease (particularly since electronic communications will to a certain extent replace current voice communications), although it will not become immediately pointless. In the longer term, however, say, in ten to twenty years, the police might have to forget about wiretapping to retrieve the content of communications altogether. Still, traffic analysis will always be possible. Indeed, to quote the Minister of Justice when she defended Dutch wiretap policy: “wiretapping concerns much more than only the contents of the conversation. *Regardless of applied cryptography*, the tap will remain useful.” [25533, nr 5, 137, italics added]

Moreover, not all criminals would use cryptography, just as nowadays not all criminals are careful what they say over the phone. It may depend for a considerable part on the future development of the communication infrastructure to what extent end users will widely employ cryptography as an add-on, or whether the security features of the communication infrastructure will be considered adequate by the vast majority of information citizens (including the less wary or over-self-assured criminals), just like they trust the telephone network today. In the former case, wiretapping would become virtually useless, but in the second case, it would likely still retain some effectiveness, albeit less than today.

Likewise, computer searches will become increasingly difficult. Although programs for file encryption will not spread so quickly as communications crypto products, they will be provided for by many operating systems. Moreover, word-processor programs, which currently use weak encryption, may shift to stronger encryption, and may build in a feature for automatic file storage in encrypted form. Disk encryptors will soon be efficient enough to encrypt the hard disk continuously, without any trouble to the user. This suggests that, like wiretaps, computer searches will become ever less effective, and may in the long term be of little use at all. With stored encryption, there will always remain chances of finding passphrases written down, and cryptanalysis and practical attacks will be more viable to crack stored encrypted data than they are with encrypted communications. (Note that there is not a severe time constraint like in wiretapping, which allows more opportunities to investigate practical attacks (see 4.5.3)). However, computer files will become more pervasive in the near future, as ever more people are using computers for daily affairs as well as business. The importance of computer searches will therefore increase in relation to physical searches. The possibility of cryptanalysis or a lucky passphrase find may not outweigh the increasing importance of stored encrypted data. So, even if there remain some chances of decrypting encrypted files found in a search, overall, law-enforcement searches will be crippled by cryptography.

There is another side to the effects of doing nothing, however. The spread of cryptography will also help law enforcement, because it will protect the information society. One of the beneficent uses of cryptography is its ability to prevent information crimes, such as computer crime, economic espionage, and counter-measures by criminal organizations to eavesdrop on the police (see 3.2.2). In this respect, law enforcement will benefit from inactivity by the government to restrict the use of cryptography. One cannot say that this positive effect ‘balances’ the negative effects of cryptography for law enforcement, since the effects are disparate, but even so, governmental inaction has its advantages for law enforcement as well.

The positive effect for law enforcement holds, of course, all the more so for the information society at large. It will benefit from the growing use of cryptography by all layers of society, in all layers of the information infrastructure. Given the necessity of cryptography to safeguard information security, not restricting crypto use may be deemed vital to the development of the information society (see 3.2). Indeed, the unrestricted market development of robust crypto systems without complicated and risky LEAK features will reinforce information security and privacy protection, while refraining from implementing legally controversial decryption demands or investigation measures respects fundamental tenets of the rule of law.

## 10.2. Applying the criteria

The zero option does not infringe privacy and the right to confidential communications, the right to a fair trial, the rule of law in general, or the right to economic development. Indeed, it is by and large beneficent for these principles, since the unrestricted, market-driven development of cryptography and crypto use will promote the information society. Needless to say, the zero option is also workable, internationally compatible, and technologically sustainable.

However, the zero option does infringe one fundamental principle: the effectiveness of the rule of law, in particular the principle that crimes must be punished. Crypto use will increasingly hamper investigation, and so, more criminals will escape justice.

Figure 10.1 gives a simplified illustration of how the zero option matches the principles.

<i>principles</i>	<i>options</i>	<i>zero option</i>
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 10.1. Zero option and principles*

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

### 10.3. Conclusion

If nothing is done, law enforcement may lose two valuable investigation tools. Wiretaps (for content) and, to a large extent, searches will be ever less effective; in the middle to long term, they may even become largely useless, depending on the future development of the information infrastructure. On the other hand, the continuing spread of cryptography helps law enforcement in that it will prevent information crimes. For society at large, a decision by government to do nothing on the crypto problem will have many benefits in terms of robust information security. The zero solution is therefore a viable option – but it must be a conscious decision by the government after a careful balance of the consequences of this and other options, not a failure to take a decision.

