

## Summary

### **The crypto controversy. A key conflict in the information society**

Noordwijkerhout (Netherlands), August 1998 – In the information society, information and, consequently, information security are growing more and more important. Therefore, there is an increasing need to employ cryptography: programs which make data inaccessible to unauthorized people. On the other hand, there is an increasing concern that criminals can use this cryptography to effectively escape the notice of police. So, cryptography produces a conflict of interests: privacy and information security versus criminal investigation. The related discussion is strongly polarized: privacy groups and law enforcement flatly oppose each other. Behold the *crypto controversy*, one of the key conflicts in the information society.

To address this controversy, I organize a three-day conference on the Dutch crypto policy, which is to answer the question: “How can and should the Dutch government address the problem that the use of strong cryptography by criminals poses to law enforcement, taking into account the legitimate interests to use cryptography in the information society?” Attending the conference are representatives of the relevant groups of Dutch society that have an interest in a just crypto policy: Alice, an average crypto user, Bob, a business crypto user, Polly, a law-enforcement official, and Suzie, a suspect (who worries about a draconian crypto policy infringing her rights of the defense). They will have to decide upon a crypto policy that reconciles the interests of privacy and information security with the interest of law enforcement.

### **Background**

To enable the conferees to make a just decision, the organizers (Tilburg and Eindhoven Universities) have written an extensive background paper which outlines the problem and the context in which it should be seen. The paper starts with a presentation of the information society, which “will profoundly change the way we live and work”, according to European Commissioner Bangemann. As information is becoming ever more important to our life and work, an information society is taking shape in which traditional borders are blurred. Media as well as market sectors converge, state monopolies on telecommunications are abolished, and electronic commerce enables customers and enterprises to do business through other intermediaries than retail shops. This society is global by nature, and national and jurisdiction borders are rapidly becoming less relevant as the Internet is booming. In this society that depends for a large part on information, the need for information security is a primary one. The confidentiality, integrity, and availability of information (the CIA of information security) must be safeguarded by a mixture of physical, organizational, technical, and legal measures.

One of the key technologies for establishing information security is cryptography, systems which use mathematical algorithms and digital keys to encipher data in such a way that only

authorized people can decrypt and read them. Especially public-key or asymmetric cryptography, which was developed in the 1970s, has opened up a vast array of applications for wide-scale encryption. (In public-key cryptography, users have a key pair consisting of a private and a public key. By widely distributing the public key – which does not require a secure channel – people can safely communicate with any number of others.) Crypto-graphy is employed to protect, e.g., telecommunications, personal data, electronic payment systems, intellectual-property rights, sensitive government and business data, and human rights. Also, cryptography can prevent crime, like computer crime and economic espionage.

A drawback of cryptography, however, is that criminals can use it to escape the notice of wiretapping and computer-searching police officers. Uncrackable crypto systems are easily available, and if criminals use them correctly (that is, if they are careful with their passphrases), they can communicate securely and store incriminating information safely without risk that the police be any the wiser. Therefore, cryptography will hamper the investigation of crime, in particular of organized crime, business crime, and computer crime. Today, the problem is not large: in the few cases that police have encountered encryption, they could generally crack it or find enough other evidence to make a winning case. However, the general expectation is that cryptocriminal use will rise significantly as cryptography is becoming ever more widely available and more user-friendly, particularly once it is built-in in the information and communications infrastructure. Since wiretapping and searching computers are important investigation measures (law-enforcement officials call wiretapping a crucial investigation technique, even if the efficacy of tapping is sometimes disputed), the threat of cryptocriminals to the rule of law is a real one. There is therefore a legitimate public interest in countering the (future) negative effect of crypto-graphy on law enforcement. In the Netherlands, this can best be addressed in the context of the general revision of investigation measures, which is taking place as a result of the finding in the mid-1990s that investigation practice had gotten out of hand ('IRT-gate').

The problem of cryptocriminals is being studied in many countries. Some states have enacted legislation (France and Russia, for instance, have virtually prohibited strong cryptography, and the Netherlands has introduced a provision that requires people to decrypt, which may soon be extended to demand decryption by suspects as well), and some states (notably the UK and the US) have expressed a serious desire to restrict the application of cryptography to systems which leak information to law-enforcement. Most countries, however, are at a loss. The OECD have issued 'guidelines' for a crypto policy which in fact do not guide at all, and states seem to be waiting for each other to see what the emerging international direction will be.

This much for the background paper, which ends on a rather desperate note: “there is a general impasse in the crypto controversy debate.”

### **Procedure**

To break the impasse, Alice, Bob, Polly, and Suzie will have to decide which option best addresses the problem of criminals using cryptography. As this is essentially a problem of balancing conflicting interests, the conference agenda follows a procedure inspired by John Rawls’ *A Theory of Justice* which should lead to a result that is acceptable to all. A particular feature of this conference is that the conference room is covered in a ‘veil of ignorance’, which ensures that the participants do not know which position in society they themselves have in reality. Thus, although they have all relevant information at their disposal, Polly, Alice, Suzie, and Bob can not be biased by their personal preferences or the particular interests of the group they represent. This will ensure that their decision is impartial and a genuine reconciliation of interests.

The first agenda item is choosing a least advantaged group, that is, the group which has most to lose in the crypto debate, where losses are counted in terms of fundamental freedoms and not in terms of material wealth. After all, the central tenet in law is to protect the weak from the strong: “law cannot be impartial in its function of regulating order: it will have to take sides with the powerless, with those placed under custody, with those who are most threatened to be overpowered.” [Peters] If there is no option which is in all respects preferable to the others, the perspective of the least advantaged group is a good device to make a decision that does justice to this central tenet. The conferees agree that, in the Dutch context, Alice represents the least-advantaged group: her privacy, including her right to confidential communications, is at stake. Alice has more to lose than Polly, who – even if wiretaps would become useless – still has various investigation measures to catch criminals, while Suzie’s rights are sufficiently protected by the right to a fair trial as interpreted by the European Court (being a Dutch conference, it has to respect the European Convention for the Protection of Human Rights). And for businessman Bob, no fundamental freedoms are at stake. Therefore, the issue will be decided from the perspective of Alice, and so, the outcome must be the one which is most acceptable to the law-abiding crypto user.

Next, the conferees choose a set of principles, with which they can assess the options to address the crypto problem. They perceive four fundamental rights as essential to the crypto problem:

- the right to privacy (including confidential communications),
- the right to a fair trial,
- the rule of law (including the right to freedom from crime), and
- the right to economic development.

Besides, the conferees will also take into account the less fundamental, but still desirable principles of workability, international compatibility, and technological sustainability. Since the principles will conflict, the conferees also define an adjudication rule: a fundamental right can only be infringed for the sake of another fundamental right, and not for the sake of a desirable principle. And to decide which fundamental right carries most weight, the conferees agree that, if all else is equal, a principle higher on the list will be accorded more weight.

### Optional directions

To end the first day, Bob, Polly, Suzie, and Alice start with discussing which options are viable to address the crypto conflict. They discard right away the non-option of banning cryptography, since this hampers the legitimate use of cryptography and thus seriously threatens privacy and information security, while it is not at all effective in preventing criminals from using cryptography anyway. With some brainwaving, they come up with four optional directions.

- Stimulate the use of cryptography which does not hamper law-enforcement, either because it cannot be used for confidentiality, or because it LEAKs (that is, has built-in Law-Enforcement Access to Keys).
- Demand suspects to decrypt and punish them if they refuse, by either convicting them for refusing to cooperate with a decryption command (that would be a new criminal provision), or by using the refusal as evidence in the primary case (effectively reversing the burden of proof).

These first two options are in fact the only options which ensure that the police can access crypto keys and decipher the encrypted data they gathered. If it should turn out that both these options are infeasible or undesirable, the police will have to do something else.

- Look elsewhere. Thus, one can consider using ‘direct eavesdropping’ (directional microphones and bugs), monitoring electromagnetic radiation (TEMPEST monitoring), stepping up infiltration, and staging crown witnesses – these are alternative ways to gather incriminating information which are not hampered by cryptography.
- Decide to do nothing (the zero option).

The second day, Polly, Suzie, Bob, and Alice discuss the merits and flaws of the options. Stimulating the development of non-confidentiality crypto does not make the problem worse for the police, but it does nothing to address cryptocriminals either. Therefore, they do not consider it an option after all. Next, reviewing LEAK cryptography (that is, key-escrow and key-recovery systems which give Law Enforcement Access to Keys to decrypt), the conferees note that the technology is yet in its infancy and that it involves intrinsic security risks. More importantly, it is not effective to catch cryptocriminals, since (smarter) criminals will not use systems which they know LEAK to the police. It is true that the police can profit from voluntary data recovery by businesses, but the development of data recovery should be left to the market.

Now, the conferees analyze under what conditions a decryption command can be given to suspects, given the privilege against self-incrimination as interpreted by the European Court in the *Funke* and *Saunders* cases. (A decryption command can easily be given to non-suspects and generally also to corporate crypto users, Bob happily notes, so that a decryption command can at any rate be given in several cases.) The privilege is not absolute, and given the *Saunders* finding that material which exists outside the will of the suspect may be demanded, the police can demand diskettes with private crypto keys to be handed over. Whether the police can also force a suspect to give the passphrase which normally protects the key is more contentious. If the police is pretty sure that the suspect is able to decrypt (in US case-law terminology: if it is a foregone conclusion that someone is able to decrypt), a decryption command is legally acceptable. The tricky issue is, however, how to enforce a decryption command: the general punishment for a refusal to cooperate with a legal order is

three months, and this can not be enough to incite serious criminals to decrypt (with which they would risk many years' imprisonment). Penalizing crypto use 'in furtherance of a crime' is not an option, since it does not ease the proof issues it is supposed to alleviate. The two main enforcement options are therefore penalizing a decryption refusal with a substantial punishment (say, a few years), or reverse the burden of proof in order to allow the decryption refusal to be used as evidence in the primary case ("if you don't want to decrypt this, we assume it contains incriminating information"). Since the first option catches criminals the wrong way (one wants offenders to be punished for the offense they committed, not for 'cryptography abuse'), and since the second option is better targeted at serious criminals, reversing the burden of proof would be better to enforce a decryption command. However, if the fundamental presumption of innocence is to be respected, strict conditions must apply (consistent with the conditions the European Court defined in *Murray*), and the command will not be effective in many cases.

A general despondency now descends over the conference: perhaps there is no feasible way to ensure that the police can access crypto keys and decipher encrypted data they suspect to be incriminating. However, Suzie, Bob, Alice, and Polly realize with some relief that the police has other investigation powers to gather data, particularly since in the post-IRT-gate era, new investigation measures are being considered. The Dutch draft law on special investigation powers proposes 'direct eavesdropping': directional microphones and bugs which catch conversations (and, who knows, keyboard strokes) the moment they are spoken (or typed), before they can be encrypted. This power could be significantly extended to address the crypto problem, in particular by allowing the police to eavesdrop directly within homes. Another alternative investigation measure is intercepting electromagnetic radiation (TEMPEST monitoring), which can reproduce the contents of computer screens from an adjacent building or vehicle. Then again, there are other ways to gather information about, in particular, organized crime: one can infiltrate a criminal organization, or one can have an accomplice testify in court as a crown witness in return for a sentence reduction. The conferees realize that these legal measures, contrary to the technical measures of eavesdropping and TEMPEST monitoring, are far removed from wiretapping and computer searches, because this yields different kinds of information. Moreover, all measures seriously infringe fundamental rights: the first two are major threats to privacy, and the last two threaten the rule of law. None of these measures, then, is an obvious solution to redress the gap in information-gathering caused by cryptocriminals. All the conferees can say at this moment, is that direct eavesdropping is more practicable than TEMPEST monitoring and that infiltration is to be preferred to crown witnesses (which is more detrimental to the rule of law).

Perhaps, then, Suzie sighs, we should do nothing at all. If the negative consequences of the options are all larger than the positive ones, perhaps that would be the best option. The one drawback of this is, of course, that it gives cryptocriminals free play. The conferees end the second day in some confusion. They have identified which options are viable to address the crypto problem: demand suspects to decrypt and reverse the burden of proof if they refuse, step up 'direct eavesdropping' and infiltration, or decide to do nothing – but they realize that not one option is really satisfying.

**Conclusion**

A night's rest, however, clears the mind, and the conferees start to review the options with renewed vigor on the third day. Remembering the perspective of Alice, the law-abiding crypto user, as the one to tackle the problem from, they review the options again. They note, first, that all viable options are of limited efficacy, as they can only be implemented with difficulty or in a quite limited number of cases. Also, they remember from the background paper that currently, the threat of cryptocriminals is small – hardly enough to justify serious infringements of fundamental rights. Besides, the police has many investigation powers that may help to partly compensate the information loss caused by cryptocriminals. For instance, they can use telecommunications traffic analysis (which is not hampered by cryptography), infiltration, and (soon) 'direct eavesdropping'. Moreover, in some cases, they can command (non-suspect or business) people to decrypt with a reasonable chance of success. Since Alice's right to privacy carries more weight than her right to freedom from crime (for the lower limit of the latter is not at stake in any option), the conferees must be wary with options which infringe privacy but which have a limited efficacy and a poor justification in investigation practice.

Taking everything into account, the conferees choose the zero option. They thus conclude that for the moment, the Dutch government should endorse the zero option as the one which best reconciles the conflicting crypto interests.

**Future**

Since everything flows, however, Suzie, Alice, Polly, and Bob realize that in the future, this policy needs to be reviewed periodically. They speculate that, once cryptocriminals do turn out to be a serious problem for the prosecution of crime, another option than the zero option may have to be chosen. The biggest future cryptocriminal threat will most likely be posed by organized criminals, and cryptocriminals will hamper wiretapping more than computer searches. To investigate and convict organized criminals, other investigation measures hold higher promise than reversing the burden of proof, which is problematic anyway in the case of encrypted communications. Moreover, from the perspective of Alice, alternative investigation measures will likely be more acceptable than a decryption-command legislation that may have the effect of putting a strict liability on crypto use. So, they feel that alternative investigation measures are preferable to enforcing a decryption command through contentious legal constructions. Perhaps, then, the government will slowly have to adapt to the idea that wiretapping is not a panacea for the information need of the police, and to focus their resources on other, less crypto-sensitive, investigation measures.

To end the conference, the participants look back and evaluate what they have done. Having defined principles and adjudication rules, surveyed possible options, and narrowed down the list to viable options, the conferees had to decide the core problem. Using the perspective of Alice as the least advantaged group, they found that for the time being, the zero option is preferable. Policy makers should, however, continue to closely monitor developments, in order to periodically review and if necessary to adjust this decision. Depending on the crime rate and the crypto use by criminals, and depending on the investigation powers the police can use, this could lead to allowing more alternative investigation measures to counter the possibly decreasing efficacy of wiretaps and computer searches.