

## Chapter 11. Reconciling interests

*The proofreader nodded, 'You see, you cannot draw lines and compartments, and refuse to budge beyond them. Sometimes you have to use your failures as stepping-stones to success. You have to maintain a fine balance between hope and despair.' He paused, considering what he had just said. 'Yes,' he repeated. 'In the end, it's all a question of balance.'*

*(Rohinton Mistry, A Fine Balance)*

The crypto conflict is a clash of legitimate interests. Privacy and information security conflict with law enforcement and national security; individual interests conflict with collective interests. I have reviewed several options to address the crypto problem for law enforcement: law-enforcement access to keys, demanding suspects to hand over keys, alternative investigation measures, or doing nothing at all. All options have positive and negative sides for differing concerns; there is no option which is a uniformly optimal solution.

Perhaps the key issue at stake is the question who controls the power to safeguard information. If cryptography is widespread, it will be the users who can protect their information – against crooks as well as against their government (which, in some countries, may occasionally coincide, for that matter). If crypto use is restricted, through promotion of LEAK crypto or through penalizing crypto use 'in furtherance of a crime', it will be the government who can wield the power to decide which information may be protected, and which information must be revealed. The delicate balance between government and citizens is at issue here. In a society where information becomes ever more important, this is a key issue indeed. This balance of power between government and citizens is intricately related to the balance in the crypto controversy. And so, we arrive at the ultimate question: how must we balance the interests of information security and privacy with the concern of law enforcement? How do you choose the option, or combination of options, that best reconciles the interests at stake?

I look at *A Theory of Justice* by Rawls as a source of inspiration. Rawls addresses the problem of social justice, which differs from the crypto problem (a part of criminal justice), but his methodology offers good clues for addressing the crypto conflict. In this chapter, I shall first describe the methodology of Rawls (11.1). Then, I shall explain how his problem differs from mine, and indicate what parts of his argument I will use (11.2). I will work out these points for the crypto problem (11.3). Then, I will apply this to the Dutch situation, and see what option or combination of options may be considered to best reconcile the conflict of crypto interests in the Dutch situation, given the assumptions outlined (11.4). I will also roughly indicate how the same procedure might be applied to the situation in the US (11.5). Finally, I will reflect on the outcome and the procedure followed (11.6).

### 11.1. Rawls and social justice

In *A Theory of Justice* (1971), John Rawls follows a long line of social philosophers to present a theoretical view of how a just society functions, or rather, should function.<sup>1</sup> Rawls aims at defining a set of principles for the major institutions of society (e.g., the organization of the political system, and the distribution of material wealth). Having an essentially contractarian point of view, he uses the mental construct of a contract that everyone in society enters into to create these institutions. He defends this position against the other major school in social philosophy, utilitarianism, which holds that the organization of society is aimed at creating the largest overall benefit for the largest number of people.

Rawls follows a fascinating thought experiment to construct his contract theory. Suppose people have to decide upon the major institutions of society. Let there be representative groups to decide this. Let them be in the ‘original position’, a hypothetical construction of a situation in which people are in a position to make an informed and just decision. To prevent personal circumstances and prejudices from influencing the decision (e.g., rich people would choose purely capitalist institutions, whereas poor people would choose socialist institutions, simply because these are better for themselves, not necessarily for society), we drop a veil of ignorance over the people: they do not know to which group they belong in real life (but they may know the relevant theories or facts of society necessary to make the decision). Thus, they will make an impartial decision and choose an organization which is the best for society at large.<sup>2</sup>

However, what is good for society at large is not necessarily good for all its groups: if the rich get twice as rich while the poor get somewhat poorer, society at large may be better off, but not the poor. Rawls assumes that people will choose principles that benefit the least advantaged group. After all, if they turn out to belong to that group once the veil of ignorance is lifted, they want the principles to ensure them an acceptable minimum level of liberty and wealth. They want to avoid the risk that the basic principles they choose will worsen the position of the least advantaged. Moreover, Rawls assumes that improvements for the least advantaged benefit the more advantaged as well (or at least will not make them worse). Therefore, he argues, the people in the original position will choose the least advantaged group as the perspective from which to make the decision. Thus, the rules should be chosen in such a way that the outcome will be preferable for the least advantaged group.

In simplifying the problem, Rawls makes several assumptions. The most important assumptions relevant here are:

- strict compliance: all members of society participate in the process and will comply with the outcome;

---

1 This section is only a description of *A Theory of Justice*, not an indication of relevant issues transposable to the crypto conflict. The differences will be outlined in 11.2.

2 “The veil of ignorance makes possible a unanimous choice of a particular conception of justice. Without these limitations on knowledge the bargaining problem of the original position would be hopelessly complicated.” [Rawls, 140]

- pure procedural justice: the problem does not allow one to judge the result from an objective criterion (material justice); rather, it is a problem that has a just outcome if the process has been followed correctly; in pure procedural justice, a correct procedure leads by definition to a just outcome;<sup>3</sup>
- the problem is tailored for a ‘maximin’ solution: people will choose the solution in which the worst possible outcome is the least bad, that is, they want to maximize the minimum they will get;<sup>4</sup>
- liberties can be effectively exercised and freedoms enjoyed; having a set of liberties which you cannot exercise is not very helpful, and someone may in that case agree to less liberties if this will enable him in future to better exercise his liberties; Rawls assumes that in a long-term perspective, the liberties will be exercised [Rawls, 151-2].

Having outlined the original position and the assumptions, Rawls advances two principles which, he argues, people would choose as the primary principles to guarantee just institutions of society. He also defines a priority rule which says that the first principle takes precedence over the second.

“First Principle

Each person is to have an equal right to the most extensive total system of equal basic liberties compatible with a similar system of liberty for all.

Second Principle

Social and economic inequalities are to be arranged so that they are both: (a) to the greatest benefit of the least advantaged, consistent with the just savings principle, and (b) attached to offices and positions open to all under conditions of fair equality of opportunity.

First Priority Rule (The Priority of Liberty)

The principles of justice are to be ranked in lexical order and therefore liberty can be restricted only for the sake of liberty. There are two cases: (a) a less extensive liberty must strengthen the total system of liberty shared by all; (b) a less than equal liberty must be acceptable to those with the lesser liberty. (...)

General Conception

All social primary goods – liberty and opportunity, income and wealth, and the bases of self-respect – are to be distributed equally unless an unequal distribution of any or all of these goods is to the advantage of the least favored.” [Rawls, 302-303]

As one can see, these principles are highly abstract: they define a theoretic ‘concept of justice’ which needs to be implemented in ‘conceptions of justice’. Rawls’ major concern is with this abstract concept of justice. The thrust of his argument is that if a conception of justice follows the principles of justice, it is a just conception. Thus, for instance, capitalist

---

3 Compare this to criminal justice, which is imperfect procedural justice, as exemplified by a criminal trial. “The characteristic mark of imperfect procedural justice is that while there is an independent criterion for the correct outcome, there is no feasible procedure which is sure to lead to it.” [Rawls, 86]

4 For instance, if people can choose between living in the US, where they can become very rich but also very poor, or living in the Netherlands, where you can never get as rich as fast as in the US, but where you will never get as poor as many in the US either, with a maximin strategy, they will choose the Netherlands. Rawls cites three characteristics of problems tailored for a maximin solution [Rawls, 154]:

- it is difficult or impossible to judge the likelihood of one or the other outcome;
- the person choosing has a conception of good which makes him care little for gaining more than the minimum he is sure to get by following the maximin rule;
- the rejected alternatives have hardly acceptable outcomes.

and socialist institutions could both be just conceptions, as long as they satisfy the rules of the concept of justice (whether they do depends for a large part on the information available in the original position on the particular society and the positions of the various groups therein).

Particularly important in Rawls' reasoning is the (first) priority rule. There is a lexical or serial ordering between the principles of justice. This means that a prior principle should be satisfied first before one can turn to the next principle. First and foremost, people have the right to liberty, which can only be restricted for the sake of other people's right to liberty. Material advantages for some (or for many) can not justify infringements of liberty of others. The system must be such that the total set of liberty is the largest possible; this total amount can be restricted only if it strengthens the system as such (e.g., society may be more stable if everyone gives up some liberty to allow law enforcement to catch those who undermine society), and the liberties may be distributed unequally only if this benefits those least advantaged.

## 11.2. The crypto conflict and criminal justice

Finding a framework to reconcile the conflicting interests in the crypto conflict differs significantly from finding rules to define social justice. The crypto problem is part of criminal justice, which, as Rawls notes himself, is quite a different area. For one thing, the assumption of strict compliance is negated in criminal justice, which deals by definition with people who will not play by the rules. Therefore, in choosing rules, you will have to take into account the effect of there being certain people who will not abide by them. Also, the level of abstraction differs: Rawls addresses the philosophical problem of social justice in the most abstract sense, whereas the crypto conflict calls for solutions in practice on a much lower level of abstraction – essentially, it is finding a solution within the context of criminal justice, not justifying criminal justice as such.

Still, there are many elements in Rawls' methodology that appeal to me and which I consider usable in describing how one can reconcile the interests in the crypto conflict. Defining an original position in which representative groups have to decide upon rules or criteria behind a veil of ignorance is a helpful way of presenting the problem in an impartial way. From this framework, with the device of the perspective of the least advantaged group, one may argue for a more detailed solution, that is, deciding which option best reconciles the conflict of interests. The ordering principle is of primary importance here, and posing a lexical ordering between, first, fundamental rights and, second, appropriate but less fundamental principles is an appealing simplifying device. This lexical ordering is of primary importance to solve a problem of justice: fundamental rights can only be infringed because of other constitutional rights, and only if they are satisfied can one look at less fundamental (or more materialistic) principles.

In the crypto conflict, it is not the case that improvements for the least advantaged group will also improve the situation of those better advantaged – improving the legal protection of suspects may decrease the freedom from crime of law-abiding citizens, and vice versa. However, the perspective of the least advantaged group is a useful device – indeed, it is at

the core of justice itself. One of the basic tenets of justice 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, 13 ] Therefore, the least advantaged group can be regarded a key device in judging conflicts of interest in criminal justice.

In presenting this analysis, I look at the problem from a Dutch perspective, since I do not consider a supranational joint approach realistic (see 1.3.1). This Dutch perspective implies several assumptions. For one, I am not extremely concerned about abuses and excesses by the police or by the threat of a police state; despite the bad example of IRT-gate, I consider in general that there is such a level of rule of law in the Netherlands that we can adequately deal with such excesses. The Dutch generally have a fairly high level of trust in their government.<sup>5</sup> I am concerned about privacy, given the process of individualization taking place on the one hand, and the increasing push of commerce and the government to infringe upon informational privacy on the other hand. Another assumption is the level of crime in the Netherlands, which, although ostensibly serious, is not particularly alarming. There is a considerable level of organized and business crime, but this does not presently threaten the rule of law or the stability of society. The concern is to check growth of crime rather than to significantly decrease it. Lastly, a basic assumption is the aim of the Dutch government to make the Netherlands an information gateway to Europe: the Netherlands wants to be at the forefront of the information society, which implies that information security is of crucial concern.

### 11.3. Description of the problem

#### 11.3.1. The original position

Into the original position, I input the relevant information on the present-day information society, cryptography, and cryptocriminals.<sup>6</sup> We are in a process of establishing a society in which information is one of the most valuable goods. Information security therefore is crucial, and cryptography is a necessary tool to achieve this. Cryptography may soon be built-in in the information infrastructure. If telecoms providers build in cryptograph, they have to ensure its decryptability to comply with wiretap obligations.

There is a considerable level of crime, in particular organized crime; business crime and computer crime are also of concern. The smarter and more sophisticated criminals, notably the organized and computer-literate ones, are increasingly using state-of-the-art technology

---

5 Having read many Amnesty International reports, I know this is a strong assumption. In most other countries, indeed in several Western European countries, the risk of police abuses should be considered (much) more serious.

6 “The notion of the rational and impartial application of principles defines the kind of knowledge that is admissible.” [Rawls, 200] The crypto problem is a legislative rather than a constitutional or philosophical problem, and so, the participants to the crypto conference have much more information on the particulars of their society than Rawls allows those in the original position to have when they choose principles of justice. [See Rawls’ four-stage sequence, 195-205.]

to escape the scrutiny of law enforcement. Cryptography is a tool they have just discovered, and are likely to use more in the near(er) future to shield their communications (particularly e-mail) end-to-end and to protect their stored data. The police can crack and attack encrypted data to some extent, notably through practical attacks against weaknesses in crypto use, but a considerable part of the ciphertexts will remain inaccessible to them.

The police has several investigation powers: search and seizure, wiretapping, and infiltration, for instance. Soon, they will most likely also be able to use direct eavesdropping and other special investigation powers, and perhaps, in a few cases, crown witnesses.

In this setting, I organize a conference in Noordwijkerhout with representatives of relevant parts of society. They have to decide upon a crypto policy that reconciles the interests of privacy and information security with the interest of law enforcement. They have all necessary information at their disposal, including the extent to which cryptography hampers law enforcement. The conference will have to answer the following 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 needs to use cryptography in the information society?

### 11.3.2. Representative groups and their veil of ignorance

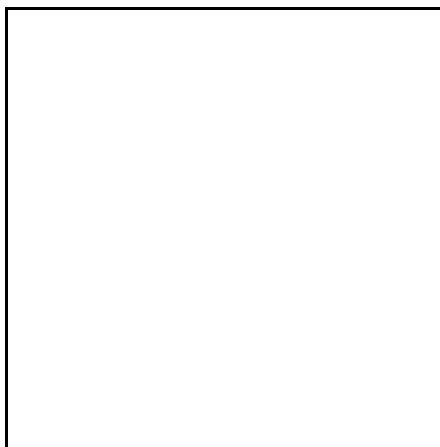
Attending the conference are:

- Alice, a law-abiding crypto user,
- Bob, a business crypto user,
- Polly, a law-enforcement official, and
- Suzie, a suspect.

Also attending, as a listener, is Carol, a crypto-using criminal and delegate of a criminal organization. She has an interest in the crypto policy to be established, but she will not play by the rules which will be decided here. Carol therefore has no voting right, but she is attending the conference as a naturally interested observer, sitting in the gallery. Note that the crypto industry is absent. They have an interest in the conference, of course, but this is not of the same order of magnitude as the interests of

Alice and Bob, which are more fundamentally at stake than the interests of a minor part of industry (cf. the lexical ordering of the principles at stake).

The attendants have names and functions, but in the process of resolving the issue, they will not know who they are. We drop a veil of ignorance over the conference table, so that not even the attendants themselves know which group they represent.<sup>7</sup> (The veil does not




---

<sup>7</sup> More generally, “any knowledge that is likely to give rise to bias and distortion and to set men against one another is ruled out.” [Rawls, 200] The veil of ignorance does allow a lot of information on the particular details of the crypto problem, but not about how each participant is positioned in the information society. Thus, it ensures impartiality.

cover the gallery – the ones around the table know they are not Carol; in reality, they may be Suzie, however.)

The academics are absent from the conference. Since they devised the procedure to ensure a just outcome, they do not need to participate in the process. The veil of ignorance ensures an impartial decision: “It enables us to say of the preferred conception of justice that it represents a genuine reconciliation of interests.” [Rawls, 142]

## 11.4. The crypto policy conference

### 11.4.1. The least advantaged group

The first agenda item is to decide which is the least advantaged group. The conferees will want to do this, because they do not know to which group they belong in real life. If they happen to be the least advantaged person in the information society, they will want the crypto policy to have taken seriously into account the consequences for them. Indeed, the worst possible outcome of some of the options for some of the representatives are very grave: Suzie might face long-term imprisonment if the burden of proof is radically shifted, if she is innocent but forgetful; Alice might lose her online privacy if she is forced to deposit her keys; Bob may have to move his company if his business has to comply with national key-recovery rules which are not implemented internationally. This is a strong argument for treating the crypto dilemma as a maximin problem: the participants will want to maximize the minimum they will get in any situation. To ensure this, they will decide the problem from the perspective of the least-advantaged representative. Another, more fundamental, reason to choose a least advantaged group is the central tenet in law to protect the weak from the strong.

Who is the least advantaged? Not Bob, who is quite powerful – his IT business is booming indeed. One might think for a moment that Polly is a candidate for the least advantaged position, but the threat of cryptography to the entire level of catching criminals is not high enough for Polly to be greatly disadvantaged. The worst outcome for her – doing nothing and seeing wiretaps and computer searches become much less efficacious – still leaves her with many investigation measures, and with many (although not all) criminals to catch.

The choice, then, is between Alice and Suzie. Suzie has a considerable level of protection in the Netherlands (although this is somewhat being eroded for the sake of crime-fighting), and in the Dutch system of a moderately inquisitory trial, the interests of the suspect are more or less balanced with those of the prosecution. The option least favorable to Suzie, enforcing a decryption demand with a penalization of a decryption refusal or a burden-of-proof reversal, will alter this balance, but not fundamentally so. If the option is to be compatible with constitutional protection of suspects as ensured by the ECHR and the case-law of the European Court, the right to a fair trial is safeguarded, and so, Suzie has less to lose than Alice.

So, Alice really represents the least advantaged group. She may suffer privacy infringements through alternative investigation measures and through restrictions in the use of cryptography, and in the unlikely event of her being suspected of a crime, she might suffer

grave consequences if she has been careless or forgetful with her crypto keys and passwords. So, the conferees decide to judge the problem from the perspective of Alice.<sup>8</sup>

#### 11.4.2. Principles and ordering rules

Next on the agenda are the defining of principles and adjudication rules. After some brainstorming and discussion, the conferees agree upon a set of principles (cf. 6.2). After some discussion over the ordering of the principles, they present the principles as following.

- 1a. The right to privacy (including confidential communications)
- 1b. The right to a fair trial
- 1c. The rule of law (including the right to freedom from crime)
- 1d. The right to economic development
- 2a. Workability (implementability and enforceability)
- 2b. International compatibility
- 2c. Technological sustainability

The lexical ordering between fundamental and less fundamental principles is natural, because the fundamental liberties at stake take precedence over other considerations. Human rights can only be infringed because of other human rights. This means that the conferees will make a decision primarily on the basis of the human rights involved. The other principles play a less decisive role, mainly when two competing options cannot be clearly decided on the basis of the primary principles.

Within each set, the ordering is less evident. The human rights of the first set are interrelated and interdependent; no human right takes precedence over others (the right to life does, but that is not at stake). It “is important to recognize that the basic liberties must be assessed as a whole, as one system. That is, the worth of one liberty normally depends upon the specification of the other liberties, and this must be taken into account in framing a constitution and in legislation generally. While it is by and large true that a greater liberty is preferable, this holds primarily for the system of liberty as a whole, and not for each particular liberty.” [Rawls, 203]

Each human right has a primary interested party: Alice for the right to privacy, Suzie for the right to a fair trial, Polly for the rule of law, and Bob for the right to economic development. This is not to say that these rights are only important for their primary interested parties – all human rights pertain to all people. However, the argument for choosing the least advantaged group does suggest to order the rights according to their primary interested party. Therefore, the conferees order the rights as pertaining to Alice (1a), Suzie (1b), Polly (1c), and Bob (1d), that is, from weak to strong. This (sub)ordering is not lexical: options should balance the principles 1a-1d rather than satisfy the first principle, the

---

8 On a European level, one may address the problem by allowing a change in the protection of suspects as an option, that is, in fact, changing the European Convention for the Protection of Human Rights and Fundamental Freedoms. This is not realistic (nor desirable) at present. If one were to do so, one should probably consider Suzie the least advantaged person, since she has much to lose in that case. This would be a different conference, though, with a European crypto policy on the agenda rather than a Dutch crypto policy.

right to privacy, to the maximum extent. It does indicate, however, a certain weight attached to the principles, so that, other things equal, a higher principle will have more weight.

The ordering in the second set is less important, since the principles matter less. It seems logical to first look at whether an option is workable in the first place, before you look at its viability in the international context or its technological sustainability. Given the strong international component of the crypto problem, international compatibility is a more valuable asset than technological sustainability. One might say that a state has more control over technology than it has over the policy of other states (the US may be an exception here). In deciding upon this ordering, the conferees have chosen the following adjudication rules.

1. A solution should satisfy the set of human rights principles to the maximum extent possible. Only if this rule is indecisive, the second set of principles should be taken into account.
2. Within each set of principles, higher principles have more weight than lower principles, other things equal.

#### **11.4.3. Selecting the options**

In the afternoon, the conferees survey the available options. Discarding right away the non-option of a crypto ban, they briefly discuss all options, ranging from cryptographic measures, demanding decryption, and alternative investigation measures to the zero option. They define the options as follows.

##### *Option 7.1 Stimulate the development and use of non-confidentiality cryptography*

The government stimulates crypto developers to make crypto systems that can only be used for safeguarding integrity and authentication, not for confidentiality. The government stimulates users, notably businesses in e-commerce, to use such products, which can be used in all layers of the information infrastructure. They mainly see to communications, not to data storage. If reliable and secure non-confidentiality systems are available, then the government may consider requiring telecoms providers who build-in authentication and integrity functions in their networks or services to use only non-confidentiality cryptography for this.

##### *Option 7.2 Stimulate the development and voluntary use of key-escrow or key-recovery systems for data storage and for the telecommunications infrastructure*

The government stimulates the development of data-recovery services that meet business needs for recovering stored data. The government stimulates users who store data in encrypted form to use these services. The government requires service providers offering data recovery to cooperate with law enforcement (by handing over private or session keys or plaintexts, depending on the circumstances) under legal warrant.

The government stimulates crypto producers to develop key-escrow or key-recovery systems for telecommunications applications, that is, products for confidential communications that allow prompt and automated law-enforcement decryption under warrant (through key deposits or tagging along recoverable session keys). The government stimulates telecoms providers who build-in cryptography in their networks and services to use such products.

##### *Option 8.1 Penalize a refusal to decrypt*

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

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

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

*Option 8.2 Penalize crypto use if this obstructs investigation*

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

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

*Option 8.3 Shift the burden of proof*

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

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

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

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

*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.

*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.

Now, the participants to the conference indicate how each option matches the principles, and on this basis, they categorize the options as an option to consider (category I), not an option (category II), or an option which does not address the problem (category 0) (cf. Chapters 7-10). For each direction, they define the local optimum: the best option *within* the direction. Also, they look at the effectivity of the option in relation to the kind of crime (organized, business, or computer crime), and they assess whether it targets transported or stored encrypted data. They simplify their analysis in two hand-outs (see Tables 11.1 and 11.2 on the following pages).

Within the cryptographic direction (cf. the analysis in 7.7.3 and 7.7.4), they argue that to separate digital signature cryptography from confidentiality crypto is viable, but they note that it does not really address the core problem; it may help in not making matters worse for law enforcement, but it does nothing to address true cryptocriminals. (It may assist criminals in exchanging keys, but since outlawing cryptography is not an option anyway, that is no argument against this option.) Since it does not infringe human rights (indeed, it may be a stimulus to economic development), the conferees decide right away that this is something the government can consider implementing, and they refer it to their colleagues who are developing a digital-signature infrastructure policy.

The other option in this direction, voluntary LEAK through key deposits or key recovery, they discard after ample consideration, as not being effective in addressing the problem. They are threatening for Alice and Bob because they involve security risks, and do not really help Polly, because (smarter) criminals will not use them. Two partial LEAK applications may help the police, however. First, LEAK systems may be a way for telecoms providers to meet their obligations of ensuring the tappability of their networks or services if they decide to build-in cryptography. The conferees note that this potential use is in fact already covered by the general wiretap cooperation requirements (see 4.3.1), and so, they need not consider this an option to address the crypto conflict – if telecoms providers use encryption, they must ensure decryptability, and if they do not use encryption, they do not pose a law-enforcement problem. The second positive contribution of voluntary LEAK is the use of data-recovery services by businesses for stored data. The conferees note that the effectiveness for law enforcement of such schemes is quite limited, since it targets only stored data in business crime. In fact, for these particular cases, the police already has sufficient powers to retrieve stored data: practical attacks to crack ciphertexts are of considerable value here (see 4.5.3), and the police can usually command business people to decrypt (see 8.2 and 8.3). So, additional stimulation of data-recovery services does not really provide extra help to the police; the government can leave it to the market to take care itself of the business need for data recovery.

Next, the participants review the direction of demanding suspects to decrypt (cf. Chapter 8). They agree that penalizing a refusal to decrypt is preferable to penalizing crypto use which hampers investigation, since the latter does not ease the proof issues it is supposed to target (the primary offense should still be proven without the ciphertexts, otherwise a con-

<i>options</i>	separate digital signatures	voluntary LEAK	penalize decryption refusal	penalize criminal crypto use	reverse burden of proof	direct eavesdropping	tempest	more infiltration	crown witnesses	zero option
<i>principles</i>										
1a privacy	+	-	±+	±+	+	-	-	+	+	+
1b fair trial	+	+	±-	±-	-	+	+	±	±	+
1c rule of law -effectiveness	-	-	+/ $\pm$	+/ $\pm$	+/ $\pm$	±	±-	±-	±-	-
-general	+	+	-	-	-	±+	±+	±	-	+
1d economic development	+	-	+	+	+	+	+	+	+	+
2a workable	±	-	+/ $\pm$	+/ $\pm$	+/ $\pm$	±	±	+/ $\pm$	±	+
2b international	±	-	+	+	+	+	+	+/ $\pm$	+	+
2c technology- neutral	±	-	+	+	+	+	±-	+	+	+
<i>overall estimate</i>	0	-	±-	-	±	±-	-	±	±-	±
<i>ranking</i>	0	II	I	II	I	I	II	I	I	I

Table 11.1. Options matching principles

-	<i>infringes principle</i>	0	<i>does not address the problem, refer elsewhere</i>
±	<i>has mixed effects, infringes to a smaller extent</i>	I	<i>option</i>
+	<i>does not infringe principle</i>	II	<i>no option</i>

viction for criminal crypto use cannot itself be proven). Penalizing criminal crypto use is therefore not an option.

They have some difficulty in choosing between the former option and reversing the burden of proof. Looking at the effect on Alice, the main difference is that penalizing a decryption refusal under weaker conditions is somewhat more privacy-infringing, since it puts a strict liability on crypto use (which may prevent people from using crypto as extensively as they would otherwise do). This liability is less in the burden-of-proof reversal, since the probable-cause requirement will better shield law-abiding Alice against investigations in which she would have to decrypt (cf. the analysis in 8.8.3, particularly under 1a and 1c, and 8.8.4). On the other hand, the penalization of the refusal to decrypt is somewhat more effective, for the same reason (more criminals will be convicted because of the lower proof requirement, albeit it not for the primary offense). From Alice's point of

<i>options and measures</i>	separate digital signatures	voluntary LEAK	penalize decryption refusal	penalize criminal crypto use	reverse burden of proof	direct eavesdropping	tempest	more infiltration	crown witnesses	zero option	wiretapping	computer search	crack/ practical attacks	ask others to decrypt
<i>applicability</i>														
organized crime			x	x	x	x	x	x	x		x	–	–	
business crime	x	x	x	x	x	x	x				–	x	x	x
computer crime	–		x	x	x	–	x	–			x	x	–	
transport/ alternative to wiretapping	–	x		–		x	–	–	–		x			
data storage/ alternative to computer search		–	x	x	x		–		–			x	x	x

Table 11.2. *Applicability of options and measures*

x applicable to a substantial degree

– partially applicable

view, penalizing a decryption refusal catches criminals the wrong way, and might sooner lead to catching the wrong criminals than a burden-of-proof reversal risks doing. Indeed, reversing the burden of proof under weaker Murray conditions is better targeted at catching the most serious and calculating criminals (especially if one takes into account a *Garantenstellung*). Here, Alice's individual right to privacy prevails over her collective right to freedom from crime by seeing criminals convicted. The conferees therefore find that the burden-of-proof reversal is the local optimum of this direction. They note, however, that the effectiveness of this option is, at best, not great.

Next, the conferees look at alternative investigation measures (cf. Chapter 9). The conferees assume that the law on special investigation powers is enacted, and thus, that direct eavesdropping is allowed under strict conditions. Comparing the option of more direct eavesdropping (i.e., weakening the conditions, within homes) with TEMPEST monitoring, they agree that the latter is technically more problematic and less practical, and that it will in general be less effective than the former. In fact, they feel that TEMPEST monitoring would be so little effective in practice, that it can not outweigh the privacy infringement on the basis of the crypto problems for law enforcement.

Reviewing infiltration and crown witnesses, they discuss their respective merits for the fundamental principles; infiltration is somewhat more privacy-infringing, whereas crown witnesses are more detrimental to the general principle of the rule of law. On the other hand,

the difference in privacy infringement is negligible, since the likelihood of such an infringement is very small in any case; Alice will not adjust her expectation of privacy if she knows that the police will use more infiltrators. Since infiltration is more effective than crown witnesses (they can be used in more cases), Alice would prefer that, although she does not want to discard the option of crown witnesses altogether – they may work in other cases than infiltration.

In the tea break, Bob mentions the subject of data mining. The others feel that it is a fascinating technology with a large potential for law enforcement, but they agree that it is not related to the crypto problem. So, they refer it to a partner committee analyzing the information policy of the judiciary.

After the break, the participants discuss whether any one alternative investigation measure is preferable over the others. Here, they get somewhat confused. On the one hand, the two preferable options (direct eavesdropping and infiltration) are applicable in more or less the same broad categories of crime: their main application is organized crime, although direct eavesdropping may also be useful in investigating business crime (but note that eavesdropping is generally less important to investigating business crime). Also, they only provide (to some extent) an alternative to wiretapping: they can reveal what criminals talk about among themselves, and – related to that – what they do. The measures cannot be regarded as useful to replace computer searches. On the other hand, direct eavesdropping is closely related to wiretapping, whereas infiltration is far more removed from the crypto problem, and consequently, their effectiveness for the police will differ considerably. One cannot say that one measure is generally more effective than the other. It is therefore quite difficult to argue whether one can compare these options, or whether one should leave them on a par, and see in each particular case which measure is more appropriate. For the moment, then, the conferees leave the options on the agenda for further consideration and comparison with the other optional directions.

But wait, Bob suggests, what would happen if we do nothing? (Cf. Chapter 10.) Having the elegance of being a very simple option which leaves most principles unharmed, the conferees see only one drawback: it does not help solve the problem. That is a major drawback, conflicting with the principle of the rule of law; criminals should, after all, be caught. By this time, the conferees have become rather despondent over the attractiveness of the options considered so far, all of which have their negative sides, and so, they are not yet convinced that they should act at all. Thus, they keep the zero option as one to consider as well.

At the end of the day, the conferees have thus limited the problem significantly, as illustrated in the following table (see Tables 11.3 and 11.4).

<i>options</i> <i>principles</i>	reverse burden of proof	direct eavesdropping	more infiltration	zero option
1a privacy	+	-	+	+
1b fair trial	-	+	±	+
1c rule of law -effectiveness	+/ $\pm$	±	$\neq$ -	-
-general	-	$\neq$ +	±	+
1d economic development	+	+	+	+
2a workable	+/ $\pm$	±	+/ $\pm$	+
2b international	+	+	+/ $\pm$	+
2c technology- neutral	+	+	+	+
<i>overall estimate</i>	±	$\neq$ -	±	±

*Table 11.3. Options to consider and principles*

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

<i>options</i> <i>applicability</i>	reverse burden of proof	direct eaves- dropping	more infiltration	zero option	wire- tapping	computer search
organized crime	x	x	x		x	-
business crime	x	x			-	x
computer crime	x	-	-		x	x
transport/ alternative to wiretapping		x	-		x	
storage/ alternative to computer search	x					x

*Table 11.4. Applicability of options to consider*

- x *applicable to a substantial degree*
- *partially applicable*

#### 11.4.4. Narrowing down the problem

The next day, the conferees look at the hand-out with the table of options to consider. They note that the principle of economic development is not a distinguishing criterion: all options score equally well on this principle. Therefore, they can leave it aside.

They also see that the less fundamental criteria do not yield fundamentally different results for the various options, having rather minor differences. The main difference is the workability, in particular the enforceability, which is not optimal for the burden-of-proof reversal or infiltration. In fact, the main problems of enforceability for these options have to do with the effectiveness and the rule of law: both options cannot be enforced completely, and thus not be completely effective, unless by infringing upon the rule of law (e.g., by radically shifting the burden of proof, or by using criminal infiltrators). This trade-off in enforceability, then, can be taken into account when discussing the primary principle of the rule of law. As to implementability, infiltration is less implementable because of the high costs involved, and the limited number of cases in which it is a valuable and valid investigation measure; direct eavesdropping is less implementable because of technical requirements and the risks of discovery; and the burden-of-proof reversal has implementation problems in that it is hard to trade-off effectiveness with the rule of law in specifying the conditions allowing it. So, in effect, all these implementation arguments can be taken as arguments in judging the effectiveness of these options. This way, the conferees can subsume the less fundamental principles under the fundamental principles. Indeed, the adjudication rule says anyway that the conferees should judge the problem by the fundamental principles first. So, they can leave aside the set of less fundamental principles and focus on the first set only.

This yields the following – simplified – decision table.

<i>options</i>	<b>reverse burden of proof</b>	<b>direct eaves- dropping</b>	<b>more infiltration</b>	<b>zero option</b>
<i>principles</i>				
1a privacy	+	–	+	+
1b fair trial	–	+	±	+
1c rule of law				
-effectiveness	+/ $\pm$	±	$\neq$ –	–
-general	–	$\neq$ +	±	+

*Table 11.5. The decision table*

– *infringes principle*

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

+ *does not infringe principle*

#### 11.4.5. The key decision

Having come this far, the conference has defined the core of the problem. Reconciling the interests in the crypto conflict really means making a decision on the basis of this table. To

do this, one does not only need a perspective from which to argue for a decision, but one also needs sufficient information on which to base the decision.

It is here that rabbits are put into the hat. The perspective is one such rabbit, and another is the information one uses. These are closely related rabbits. Depending on your perspective, you extract different information from the same data. For example, suppose that cryptography hampers investigation in 20 per cent of all cases involving wiretaps, and that in 60 per cent of these cases, the investigation does not lead to a conviction. Now Bob will argue that cryptography does *not* hamper investigation in 88 per cent (80% plus 40% of 20%) of all wiretap cases, and in the 12 per cent in which it does, who says that without cryptography there would have been enough evidence anyway? Polly, on the other hand, will argue that 12 per cent of all wiretap cases is quite significant (over 400 cases a year), and, moreover, these 12 per cent will likely include the most intelligent and serious criminals, who pose the biggest threat to society. This way, one's perspective can effectively steer one's 'knowledge' and the way one interprets data.

Therefore, I argue that the perspective in judging the dilemma is tantamount, and that this is the main rabbit one puts in the hat. In my case, the rabbit is Alice. I have argued that she is the least advantaged party in the discussion.<sup>9</sup> Therefore, the conferees will look at the decision table from her perspective, which means that in principle, they will rate privacy higher than the effectiveness of a solution. The base-line is a level of the rule of law which Alice, the everyday crypto user, considers acceptable. She does not want to live in a society ruled by criminals; nor does she want to live in a police state. She will measure "the danger to the liberty of the representative citizen measured by the likelihood that these sanctions will wrongly interfere with [her] freedom. The establishment of a coercive agency is rational only if these disadvantages are less than the loss of liberty from instability." (Rawls, p. 241)

First, Alice remembers that all (active) options are implementable, but in a limited way: they can only solve a small part of the problem if they are not to do away with the rule of law at all. Reversing the burden of proof under Murray conditions can be successful in only a very small number of cases where stored encrypted data hamper investigation. Allowing direct eavesdropping under less strict conditions may yield extra wiretap-replacing information in some cases, but the additional value of lowering the conditions can never redress the information loss in the bulk of crypto cases. Likewise, stepping up infiltration will only yield a quite limited additional source of information for the police.

Moreover, living in the Netherlands, Alice does not currently perceive cryptocriminals as a severe threat to her living. The information she has available does not indicate that (the baseline of) the rule of law is really threatened. For one thing, serious criminals are still being convicted, and there is no indication that there is a significant market segment of criminal organizations which escapes law enforcement through cryptography.<sup>10</sup> Indeed, the number

---

9 Note that it is the choice of Alice as the least advantaged group which is a rabbit, not the device of the least advantaged group as such.

10 The press release of the Public Prosecutor on its publication of the 1997 annual report rings optimistic about its investigation of organized crime. "Moreover, in 1997, the Public Prosecutor has successfully brought before the court the top of a number of important gangs. Besides, much attention has been paid to setting up and expanding the information position. For this, more and more varied channels are being tapped to collect (criminal) information." [OM 98]

of cases in which cryptography is blocking cases is currently very low (4.5.2). One can expect this to increase in the future, but to what extent this will be so remains to be seen – this may for a large part depend on how the information infrastructure develops, with either built-in cryptography or with a security infrastructure that depends more on end-to-end encryption. In any case, there will always be criminals who will not use cryptography, just as currently there is a significant number of criminals who use tappable phones despite the common knowledge that they run a risk of being overheard.

Also, if Alice looks at the information available to her in the original position, she sees that the police has quite a few tools available to continue retrieving information in the course of investigation. For one thing, the police can try practical attacks to decrypt stored data, or – if the encrypted file seems important enough – they may even try a brute-force attack on a supercomputer or through a distributed attack (cf. 3.1.4-5). Current experience seems to indicate that such attacks have a significant chance of success (4.5.3). Also, in some cases, the police can command people to decrypt, notably in business crime cases when the privilege against self-incrimination does not hold (8.3), or when the business uses a data-recovery service. Alice also notes that when network and service providers use encryption, they are already required by law to provide the original signal. Besides, traffic analysis is an important part of gathering information in transport, and this is not hampered by cryptography. Then again, the police have other investigation measures at their disposal, which can satisfy some of their need for knowledge. Infiltration is a good alternative to gather information and evidence on criminal organizations, although the high costs limit its potential. Direct eavesdropping will most likely soon be allowed, even within homes for very serious crimes, and perhaps crown witnesses will appear on the court stage soon. These alternative investigation measures may to some extent replace the use of wiretaps (note that options 9.1 and 9.3 do not concern the use of direct eavesdropping or infiltration as such, but they involve lowering the conditions for their use to make them more investigation-friendly).

Judging from this information, Alice decides that the current threat of cryptocriminals is not enough to justify infringing fundamental rights by enacting one of the (non-zero) options. The blocking of computer searches can be addressed by practical attacks and by demanding others to decrypt – the potential small extra value of a burden-of-proof reversal (option 8.3) cannot outweigh the detriment to the rule of law. The decrease in wiretap efficacy can to some extent be met by other investigation measures currently allowed; the potential extra infringement of privacy and the rule of law if the conditions for such measures are weakened (options 9.1 and 9.3) cannot be justified by their marginal additional value to retrieve still a little more information.

There will no doubt be some criminals who will escape justice through cryptography in the next few years, but this does not alter Alice's view: she puts up with this in view of her privacy. Moreover, her intuitive sense of justice tells her that the rule of law would currently be more infringed by allowing burden-of-proof reversals or by having bugs or infiltrators become more pervasive. For the moment, Alice concludes to do nothing. The Dutch government should endorse the zero option as the one which best reconciles the conflicting crypto interests.

#### 11.4.6. Looking at the future

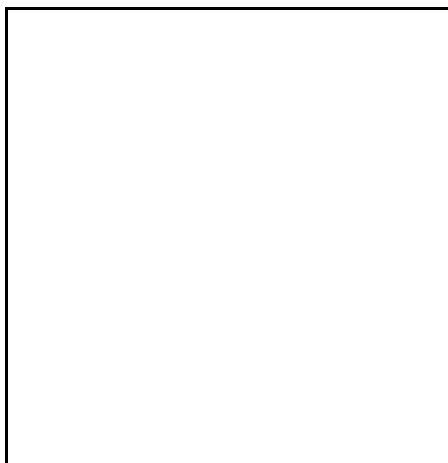
The conference participants are aware, though, that we live in a changing world, and they will continue to closely monitor developments to see whether Alice's argument still holds. They will look at the number of investigations being definitively blocked by cryptography, and they will also continue to make assessments of the overall level of crime and of the sway criminal organizations may hold over Dutch society. Besides, Alice and Polly are avid readers of the *Staatsblad* (which promulgates legislation) and the *Nederlandse Jurisprudentie* (which publishes case law), so that they can monitor the investigation powers the police have. They will take into account whether and to what extent the police can use directional microphones, bugging, TEMPEST monitoring, infiltration, crown witnesses, data mining, and other measures that may be invented and allowed in future. If the conference participants find that cryptography indeed allows criminals to escape the police more than they care for (i.e., if the base-line of the rule of law is crossed), they will reconsider the options for addressing the crypto conflict.

Then, they will again make a list of the available options. They will leaf through the latest proceedings of the CRYPTO and EUROCRYPT conferences to see what developments there are in the cryptographic field. Perhaps, new LEAK protocols or systems are being developed which are more reliable and more secure than current proposals. Also, if the market for data-recovery services will have developed over the next few years, the conferees can see to what extent individuals and businesses are using these services. If they turn out to be quite reliable and not to pose significant security risks (which can currently not be said, because such services are yet in their infancy), they could define an option to stimulate these services, or perhaps even to make them mandatory in specific circumstances (such as today there are formal obligations for keeping books). This could mean that the participants should reconsider option 7.2 (which I do not consider likely, but for a just procedure, they must take everything into account).

The option list will, of course, still contain the decryption command options, in particular the burden-of-proof reversal, and it may comprise several alternative investigation measures – new ones, or traditional ones with weaker conditions. Depending on these options and on the positions of the various representative groups, future conferences should each time decide which is the least advantaged group. For instance, if it is seriously being considered to reverse the burden of proof under weaker Murray conditions (which likely should be done on a European level, given the protection of the ECPHR), then it may turn out that Suzie rather than Alice has most to lose. Or if cryptocriminals overwhelmingly defeat the police and future IRT gates lead to a restriction of police powers, perhaps Polly will emerge the least advantaged. I consider it unlikely that in the near to middle future the decision on the least advantaged group would lead to anyone but Alice, but it is a decision which should always be carefully made. For the time being, let us suppose that Alice will still provide the perspective to judge the problem from.

To decide which of the option is preferable to the least advantaged group, the conference participants will redefine the original position. What is the exact way in which crypto blocks the investigation? Is it mostly stored ciphertexts obtained through searches that the police cannot read, or is it end-to-end encryption that defeats wiretaps? In what stage of the investigation does the police encounter crypto? The burden-of-proof reversal is targeted

mainly at stored encrypted data needed for finalizing the evidence, whereas most alternative investigation measures are more useful as a replacement of wiretaps in the earlier stages of the investigation, or, sometimes, to gather key evidence. The conference will also investigate what kinds of crime are at stake: is it mainly cryptocriminal organizations that escape justice, or is it white-collar criminals, or is computer crime soaring because of the crypto shield? Again, the exact scope of the investigation powers will be a major determinant of the original position. Depending on the definition of the original position and the perspective of the least advantaged group, the conferees can debate which option is preferable.



Currently, it is hard to predict what the conference will find in the future. Still, some judgments can be made at this stage. Enforcing decryption commands through penalizing a decryption refusal (or worse, through penalizing crypto use which hampers investigation) put a strict liability on crypto use, and it is instrumental legislation which does not lead to convicting criminals the right way. From the perspective of Alice, the law-abiding crypto user, this can hardly be desirable. The trade-off between effectiveness (convicting serious criminals who refuse to decrypt) and a fair trial (not convicting Alice if she has forgotten her key) is hard to make, as is the setting of a maximum punishment on the decryption refusal. The only viable way to enforce a decryption command, therefore, will be to reverse the burden of proof. Here, the trade-off of strict Murray conditions (ensuring compatibility with the right to a fair trial) with effectiveness will also be difficult. If a burden-of-proof reversal is to be effective in really convicting the serious criminals the option is aimed at, it can easily infringe the right to a fair trial more than the European Court will care for.

But perhaps the future will make the trade-off easier. If it turns out that the information infrastructure is a highly secure and reliable one, which Alice can trust with her confidential messages without having to encrypt end-to-end (like we currently trust the telephone system), or, more importantly, if operating systems are developed to automatically encrypt stored data in a LEAK-compliant way, so that Alice does not need to encrypt stored data herself, then a strict liability for using crypto and having to decrypt may become more acceptable. In other words, it may then be more fair to require Alice to prove that the encrypted data are not incriminating by decrypting, or, if she cannot decrypt, to argue why she used encryption in the first place. With the current confusion over crypto laws (in particular, export laws) and the rapidly changing information infrastructure, it cannot be predicted whether the information infrastructure will develop in this way. It may turn out that to realize her right to privacy and to confidential communication, Alice will have to use encryption herself, and in that case, I think reversing the burden of proof if the police encounters cryptography during an investigation is not really an option.

My feeling is that for at least several years to come, if a non-zero option is required to counter the increasing threat of cryptocriminals, the government should look at alternative investigation measures rather than at enforcing decryption commands through contentious legal constructions. It is true that a decryption command is much more closely targeted at the problem of cryptocriminals, whereas most investigation measures provide quite different kinds of information in only part of the investigation cases. Yet from the perspective of Alice, alternative investigation measures will likely be more acceptable than putting a strict liability on crypto use. This is all the more so since with stored encrypted data, the police has a considerable array of tools available to retrieve the information: practical attacks, and demanding decryption within the limits of (*Funke* and *Saunders*) case law; also, in investigating business crime (one of the important targets of computer searches), there is a larger likelihood of the business cooperating with law enforcement. The biggest future cryptocriminal threat may therefore be to wiretapping rather than to computer searches, and it will most likely be caused by organized criminals. To investigate and convict them, other investigation measures hold higher promise than reversing the burden of proof, which is problematic anyway with encrypted communications. 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.

#### **11.4.7. Evaluation**

At the end of the conference, the participants look back and evaluate what they have done. After defining principles and adjudication rules, surveying possible options, narrowing 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 seems preferable. Policy makers should continue to closely monitor developments, in order to periodically readjust this decision. Depending upon the crime rate and the crypto use by criminals, and depending upon the investigation powers the police can use, a future readjustment of the policy may be to allow more alternative investigation measures to counter the possibly decreasing efficacy of wiretaps.

What the conferees have done, is to list all viable options, then to narrow these down to the best option, given the principles, information, and perspective chosen. They have also pondered upon possible future measures, in case more is felt to be needed in future, by adding other options and then readjusting the balance. The process thus resembles a multiple hour-glass, in which the sand (all possible options) is narrowed down to the best option at that time, after which the other options are again added together with new data; then, the options may be again narrowed down to the best option at the next point of time. At each point of time, the weight of the grains of sand (the data added) and the form of the glass (the perspective from which you look at the problem) steer the outcome.

#### **11.5. Agenda for a US conference**

If the conference had been held in the US, with the aim of developing a US crypto policy, would the outcome have been different? Not necessarily, although the input would have differed considerably. A good analysis of the US situation requires an extensive research

which is outside the scope of this book. Here, I can only indicate what items should be researched and taken into account in addressing the crypto conflict in the US.

First of all, the assumptions for the Dutch situation are not directly applicable to the US. For one thing, the crime rate and the kind of criminals may differ; apart from organized and business crime, computer crime may be ahead of the Netherlands, considering the general lead the US has in the ICT field. Moreover, terrorism is a bigger concern in the US than in the Netherlands. In fact, the crypto debate centers as much on national security as on law enforcement, and the two will be difficult to treat as separate policy issues in the US. Also, one must consider to what extent crime in the US is threatening the rule of law or society at large.

Likewise, investigation powers differ as well. In the US, bugging has been used for quite some time, and crown witnesses have played their part in criminal proceedings. Law enforcement in the US seems less dependent on wiretapping (see 4.3.2). So, the specific problems cryptography poses to law enforcement in the US will to some extent differ from those in the Netherlands, at least in scope.

Another difference relates to the concern over police powers. The Dutch generally seem to have a higher level of trust in their government (including law-enforcement agents) than US citizens have – compare Mike Nelson’s constraints for an acceptable crypto policy: “Any solution the U.S. government endorses is immediately suspect” and “No one trusts anyone” [Nelson]. Related to this is a different conception of privacy in the US: “Though it may be an overgeneralization to say our European neighbors trust governments but not corporations with their personal lives while our loyalties are reversed, to some degree this pattern is reflected in each of our laws.” [Field] More in general, differences in constitutional protection in the US can lead to different weights being attached to the fundamental rights that are pivotal to the argument.

All these (potential) differences in the state of affairs imply that the input into the original position must be described differently for the US. This, of course, is a major factor influencing the outcome of the conference.

Another important agenda item in the US will be choosing a least advantaged group. I think the same representative groups should participate behind the veil of ignorance in the US conference: individual crypto users, business crypto users, law enforcement, and suspects, perhaps complemented with a national-security representative. The main factors influencing the decision which of these groups is the least advantaged are the weights attached to the various fundamental rights, the balance of power between citizens and the state, and the instruments that the various groups have to secure their powers and rights.

The principles and ordering rules I used for the Netherlands can likely be used in the US as well, perhaps with some shifting of the order of the fundamental rights within the first group of principles.

Since most alternative investigation measures I have outlined are already allowed to a certain extent in the US, the option list in the US would consist mainly of law-enforcement access to keys (which would, more generally, be government access to keys, since the national-security agencies would be the first to grasp the opportunity of accessing keys), enforcing a decryption demand, and significantly stepping up certain investigation measures, like bugging or infiltration. Of course, the zero option should be on the US agenda as well.

With these items settled, the US conferees can start debating which of the options is preferable, given the information for the original position and the least advantaged group. This will require thoughtful analysis, and the conference should take time for its decision. The procedure is in fact key to developing a crypto policy which is acceptable to all representative groups, and therefore, the conferees should carefully detail the argumentative steps they take and motivate their choices. Only with open and argued reasoning is there a chance that the still much polarized debate can be resolved in the US.

## 11.6. Conclusion

*If the scheme as a whole seems on reflection to clarify and to order our thoughts, and if it tends to reduce disagreements and to bring divergent convictions more in line, then it has done all that one may reasonably ask. (Rawls, A Theory of Justice)*

How does the outcome of the conference match, in Rawls' phrase, our considered judgments in reflective equilibrium? That the zero option is for the time being the best way (not) to act need not be surprising. That is a rather direct consequence of the rabbit I put in the hat, having chosen the average, law-abiding crypto user Alice as the least advantaged group and having looked at the various options in the original position from her perspective. It is more on the procedure that I would like to reflect: has it been a good way of reconciling the interests at stake in the crypto conflict?

There are two crucial factors in the procedure. The first is giving a good overview of the options available and judging how they meet the required principles. The second, and most important, factor is making clear which choices one makes in making a decision: how do you value the principles (that is, which adjudication rules do you use), what information do you use as input, and which perspective do you choose? These 'rabbit choices' are essential; the conjuring one performs with the hat afterwards is more show than substance. In fact, there are many ways of conjuring, but in the end, you still draw out of the hat the rabbit you used as input. Still, the conjuring matters, because it is key to making the rabbit acceptable to all interested parties.

The Rawls procedure is a good way of showing these choices and arguing for the decisions made. It has made me order the principles, and describe the information for the original position that I perceive as essential to the problem. Also, it has made me choose the perspective of the least advantaged group. The specific choices I made (the rabbits I chose) are open to discussion; I have argued for them from my point of view. The procedure is open to discussion as well, although I argue that this procedure is preferable to that used by most studies so far, which often amount to showing a rabbit and claiming this was conjured out of a hat backstage. That is not a satisfactory way to address so crucial a conflict of interests as is at stake here. The citizens of the information society have a right to know in what way their interests are balanced by the policy makers. Alice must be able to review the decision-making process, and she should be able to feel that she would indeed have made the same decision herself. Only then can she say that the outcome really reconciles her conflicting interests.