

## **Part II**

### **Framework and analysis**

## Chapter 6. Framework and set of principles

*A conception of right is a set of principles, general in form and universal in application, that is to be publicly recognized as a final court of appeal for ordering the conflicting claims of moral persons.*

*(John Rawls, A Theory of Justice)*

The crypto controversy is a problem of balance. We have legitimate interests of crypto users as well as legitimate interests of law enforcement, and they clash. Addressing the crypto problem for law enforcement means finding the right balance between all interests. But how is one to find a right balance?

Consider the following two statements. The “law enforcement community fully supports a balanced encryption policy (...) Key escrow is not just the only solution; it is, in fact, a very good solution because it effectively balances fundamental societal concerns involving privacy, information security, electronic commerce, public safety, and national security.” Thus spoke FBI Director Freeh [Freeh 96]. The National Research Council found, however, that “on balance, the advantages of more widespread use of cryptography outweigh the disadvantages,” [NRC, 300] and concluded that key escrow is not the right balance. Both claim to have carefully balanced the interests at stake, and yet they draw quite different conclusions.

Most statements, standpoints, and reports hardly give insight in the process of reaching a balance. Not even the extensive and well-researched NRC report makes clear how it arrives at its conclusion. (Perhaps it did not have to, since the report, being the product of a commission with representatives from all sides, can be seen as being balanced by definition – pure procedural justice in practice.) The OECD ‘guidelines’ for a crypto policy fail to give any indication *how* one is to balance all principles. By stating that all principles can only be implemented together as a whole, they only reiterate the problem (there are clashing interests) without indicating a solution. The OECD ‘guidelines’ thus leave it at the discretion of each government to develop a policy, and say that they have struck the right balance – which may result in such differing outcomes as those stated by Freeh and the National Research Council.<sup>1</sup> Their procedure is like conjuring a rabbit out of a hat, leaving the public with the feeling that a trick is being played.

I could do the same – present possible options to address the problem, describe pros and cons, analyze how the options affect the interests at stake, and conclude that this or that option is, in effect, the most balanced one. That is hardly an intellectually satisfying result.

---

<sup>1</sup> Compare this to what Rawls remarks about the intuitionist approach: “they include no explicit method, no priority rules, for weighing these principles against one another: we are simply to strike a balance by intuition, by what seems to us most nearly right.” [Rawls, 34]

One should clarify the process of arriving at the conclusion (and ‘balancing’ is the key to this process), if the conclusion is to have any claim to being well-founded. This sounds more self-explanatory than it is; in academic legal studies, *how* one balances is often seen as a factual process, escaping rational explanation, just as a judge’s intuitive decision whether someone is guilty or not is considered a factual and largely internal process.<sup>2</sup>

I will aim at doing more than just saying I have carefully balanced the interests. By posing a framework for balancing the various interests, I hope to make clear how one can address the crypto conflict. Into this framework, I will input assumptions largely based on the Dutch situation on which I focus. This, essentially, amounts to showing the rabbit before the conjuring starts, and to be open in the way I conjure with it, instead of conjuring up the rabbit at the final conclusion to the public’s surprise. The framework I choose will make it clear which assumptions I make and which procedure I follow. Other people favoring different assumptions and coping with other national situations can use different rabbits. It is really the conjuring that matters, not the rabbit.

### 6.1. Choosing a framework

*So for the purposes of this book, the views of the reader and the author are the only ones that count. The opinions of others are used only to clear our own heads.*  
(Rawls, *A Theory of Justice*)

For my framework, I choose elements from *A Theory of Justice* by John Rawls. I was led to Rawls by the fierce opposition in the crypto debate between the various pressure groups, each of which has been hard put to imagine that the ‘other side’ had a legitimate interest as well. This one-sidedness of both sides made me long for the ‘veil of ignorance’ that Rawls uses in developing his theory of social justice. He addresses the problem of choosing a just structure for the major institutions of society by having people choose principles behind a veil of ignorance, which prohibits them from seeing which position in society they really have. That, surely, would be a great procedure to follow here, if the police, privacy lobby groups, businesses, and citizens could discuss a crypto policy without knowing which of these groups they belong to in real life.

Whereas Rawls stands firmly on the shoulders of giant political philosophers, I have no intention of embedding my argument in legal or political theory. I use Rawls as a source of inspiration, mainly because of his lucid style of writing, his sense of justice, and his choice

---

2 “There is a need for methods to balance interests, to provide for the democratic legitimization of balancing interests, and not to do again the balancing of interests for every single case, but to generalize it as much as possible. At least in private law, there is yet but little research in which these methods are being developed.” [Barendrecht, 713]. Compare also what Jan Leijten has said about the ‘myth of the scales’: “the particular nature of the pair of scales is lacking in the administration of justice. The concrete identification of the value of the weights. I myself, in a long life as a lawyer, will also have occasionally committed the sin of expressing that I had come to the decision after and through a careful weighing of the mutual interests. But it remains a phrase that in itself is saying nothing, because we do measure or weigh two things, but only after having first identified the weight of these things ourselves” [Leijten].

of metaphors to argue his case. I have taken the liberty of pulling Rawls' metaphors out of the context of their original position, and transposed them to my crypto problem, thus altering their original meaning. So, Rawls does not serve as a methodological basis, but he gives me useful metaphors to construct a convincing (or so I hope) argument – nothing less.

Besides the veil of ignorance, the elements of Rawls I find useful in this context are his ways of simplifying the problem – which is one of the major challenges of addressing any complex problem. Rawls defines representative groups that hold the various social positions relevant to the problem; this clarifies the analysis. Then, by choosing the perspective of a least advantaged group from which to judge the problem, one can effectively simplify the decision making in a way that satisfies our intuitive sense of justice. Finally, another useful simplification is Rawls' handling of the ordering problem. If you have several principles, there must be a way of comparing these: you must identify meta-rules. Rawls greatly simplifies the problem by postulating a serial ordering, which means that the first principle should be met before the next principle can be taken into account.

Of course, Rawls' framework cannot be transposed directly to other problems. His problem, *social* justice, is quite different from the crypto problem, which is a subset of *criminal* justice. I will therefore use the framework as a source of inspiration which allows me to describe the problem and the reconciliation of the interests at stake in illuminating metaphors. I shall explain the framework and the similarities and differences with Rawls in more detail in Chapter 11. In this Chapter, I shall present the principles I consider relevant to the crypto problem. I shall define the principles I choose, first the fundamental and constitution-related principles (6.2.1), and next the more practical and technical principles (6.2.2). I conclude by indicating the way in which I shall draw upon these principles in the following chapters, and how I aim at balancing them in Chapter 11 (6.3).

## **6.2. A set of principles**

Principles should be self-evident. It does not matter where they come from or who defends them: they explain themselves. It must only be argued why they are relevant to the problem at issue. Instead of analyzing various likely sources for finding principles (for instance, the constitution, human rights treaties, principles for legislation, various definitions of principles for a crypto policy), I shall simply present the principles I consider relevant, and argue why they are relevant to addressing the crypto controversy.

### **6.2.1. Fundamental principles**

Fundamental principles concern basic human rights. These rights have to be respected by everyone, in all circumstances. They can sometimes be infringed upon, but only if the reason is sufficiently compelling; only competing basic human rights can legitimize such infringements. It is clear that a solution to the crypto problem should respect the basic human rights, although it may be less clear what rights are at stake. In my view, there are four rights that play a role, three of them dealing with civil and political rights (1a-1c), and one with social and economic rights (1d). Another useful distinction is between individual (1a-1b) and collective (1c-1d) human rights (some privacy lobby groups have a tendency of forgetting the latter).

**Principle 1a. The right to privacy, including confidential communications**

The right to privacy is based on what Judge Cooley has called the right “to be let alone” [Warren]. It is an increasingly important right: individualism is at an all-time high, and information is becoming all-important. In the information society, privacy centers on informational privacy, the right to keep your information to yourself and share it with those of your own choice.

The right to privacy is recognized in many constitutions and human rights treaties; e.g., the ECHR reads: “Everyone has the right to respect for his private and family life, his home and his correspondence.” It is not absolute, but an infringement can only take place if it is necessary in a democratic society for national security, law enforcement or the economic well-being of a state. Thus, a state can enact legislation authorizing the police to wiretap, to read correspondence, or to use other means to gather privacy-sensitive information, under strict conditions meeting the requirements of subsidiarity and proportionality.

Cryptography is one of the best tools to safeguard the confidentiality of communications and to protect stored information. A crypto policy therefore naturally has to take into account the right to privacy, including the right to confidential communication.

**Principle 1b. The right to a fair trial**

The right to a fair trial is one of the assets of a society which advocates the rule of law. It is recognized in article 6 of the ECHR, and it has been elaborated in the case-law of the European Court. Among its many manifestations are the privilege against self-incrimination and the presumption of innocence, which are relevant to the crypto conflict because of the option of asking suspects to hand over encryption keys or to decrypt possibly incriminating ciphertexts themselves (Chapter 8).

**Principle 1c. The rule of law, including the right to freedom from crime**

Every theory of law somehow tries to argue for the primacy of law over power. It means that the law is primary, not the people in power who implement the law, nor those who break the law. The rule of law is a fundamental principle in our society; as long as ‘the law’ is a just law, and it is respected by those in power, the benefits for society are evident. Since no society has solely perfect citizens, criminal law and criminal justice have to be part of any law system. I shall not go into the general and complex aspects of criminal justice; I am mainly concerned about one aspect of criminal justice, namely that cryptography enables

people to effectively escape law enforcement. The right to freedom from crime is part and parcel of the general rule of law, and it is in this sense that I shall mainly use this principle.

The rule of law means, first, that a society should try to prevent crimes, and, second, that, committed crimes should be redressed, usually by prosecuting their perpetrators. It is under this heading that I will range the law-enforcement concern about cryptocriminals: if cryptography enables some criminals to escape prosecution altogether, the principle of the rule of law is violated. That is a strong argument for infringing other fundamental rights – it is essentially here that ‘the balance’ has to be struck. This also means that other fundamental rights can only be breached as long as the infringement to the rule of law by cryptography is countered (that is, annulled, or at least significantly weakened). In other words, solutions to the crypto problem must help law enforcement catch criminals: the solution must be *effective*.

#### **Principle 1d. The right to economic development**

The right to economic development is of a different order than the previous. Still, it is a fundamental right enshrined in human rights law, primarily the International Covenant on Economic, Social and Cultural Rights. The more dependent economies become on information, the more important information security becomes for society. It is therefore relevant to the crypto debate, since cryptography is a primary tool for information security. Solutions to the crypto problem must take into account its effects upon the economy. The principle is related to the internationality principle (see below). Solutions that are not compatible on the international level tend to jeopardize the national economy: they will scare away companies to more crypto-friendly countries.

#### **6.2.2. Less fundamental principles**

There are other principles which are important to the crypto problem. They are less fundamental than basic human rights, in the sense that they should be fulfilled as far as possible, but they need not be maximized at all costs. Human rights can only be preceded by other human rights, and other principles can not override human rights.

#### **Principle 2a. A solution must be workable**

It almost goes without saying that if you choose a solution to a problem, the solution must be workable. Almost – for this principle is sometimes attached less importance by the legislature when it stresses the symbolic value of a law: even though a law can not be enforced, it may be important to have it because, for instance, it deters people. (Penalization of spreading computer viruses is arguably symbolic in that sense.)

The main thrust of the principle that a solution must be workable is that it is *implementable*: which means that it must be possible to implement it in real life, and that those who have to live up to the solution must be able to comply with it. Besides, it should also be *enforceable*, which means that there must be a way to ensure that the solution is lived up to.

The second component, enforceability, is not absolute: hardly any legislation is completely enforceable. However, there must be a minimum level of ensuring that the solution is carried out in practice. Where the minimum lies, depends rather on the situation

– speed-limit legislation is (and generally can be) only enforced by sample controls, whereas hostage-taking has a near-total level of enforcement (in the sense that everything possible is done to prevent or to punish hostage-takers). Enforceability also relates to those who are to enforce the solution: there must be ways to ensure that those who implement and control the solution do that in a just way, compatible with the aim of the solution and with other rights and duties. In this sense, enforceability of legislation also means that government and other public officials are controlled, e.g., that they do not stop cars during a speed-limit control in order to check for drugs smuggling, or that they do not use excessive force in an attempt to free hostages.

The first component, implementability, I tend to regard as rather absolute. If part of a solution can not be implemented, it should not be part of the solution, and if this unimplementable part is inextricably related to the solution as such, the solution is seriously flawed. Likewise, if there are situations in which the solution is not observable, the solution should be altered. With legislation, and particularly with criminal law, it can not be the case that there are legal consequences (particularly punishments) attached to something which someone cannot do. Of course, this is a matter of principle: a solution must be observable *in principle* in all cases in which it can be reasonably thought to be relevant, which is not to say that all persons will always really be able to comply with it.

**Principle 2b. A solution must be internationally compatible**

For two reasons, the crypto problem is an eminently international problem. First, the information society, of which cryptography is a vital part, is essentially a global society with blurred national borders. Second, serious crime is increasingly cross-border crime, with criminal organizations consisting of several nationalities and cooperating with partners in delivery or supply countries. Therefore, any solution to the crypto problem must make sense in an international context. That does not mean that the same solution should be implemented worldwide, but it does mean that a soloist solution which disregards the international nature of the problem is likely to be counter-productive.

**Principle 2c. A solution must be technologically sustainable**

The rise of the information society has posed problems for laws that are technology-specific, for instance, the power of the police to wiretap telephone ‘conversations’ (which excludes facsimile messages), the constitutional protection of ‘letters and telegrams’ (which may not cover e-mail messages), and the criminal provisions on damaging or stealing property (which do not cover data). Whereas most of such laws have been or are being adapted to the information age, the lesson to draw is to think carefully over the substance and wording of laws, and try and make them as sustainable in light of technological developments as possible.

If a solution to the crypto problem is to withstand the tooth of time (for at least, say, ten years), it must abstract from the technology. After all, modern cryptography has been around for only thirty years, and the field is still developing rapidly. A solution must assess how future developments in cryptography and its applications may impact on its lasting efficacy.

**Comparison with the OECD principles**

How do the OECD principles for a crypto policy compare to the principles I consider relevant? Note that the OECD 'guidelines' are broader in scope, dealing with crypto policy at large. They are also relevant to a policy for a digital signature (or public-key) infrastructure, and they mention national-security interests on a par with law-enforcement interests. My concern is only to devise a crypto policy to meet law-enforcement interests. Also note that the OECD principles are not serially ordered: no principle has priority over others, and they should be implemented as a whole.

The first set of the OECD principles (trust, free choice, market-driven development, and standards), and the principle of liability, relate to principle 1d, the right to economic development: all these principles define that a policy must satisfy the information-security demands of the information society. They also relate partly to principle 2c, technological sustainability. The fifth principle, privacy, and the eighth principle, international cooperation, are the same as my principles 1a and 2b, respectively. The sixth principle, lawful access, relates to principle 1c, the rule of law, as far as lawful access by government authorities is concerned. Lawful access by others I do not consider relevant to my problem. Liability, the seventh OECD principle, is partially covered by principle 2a, enforceability, since liability should be addressed to make sure that crypto users – and law-enforcement agents – can observe the policy (this is mainly relevant to key-recovery solutions, see Chapter 7).

my principles	OECD principles
1a privacy	5 privacy
1b fair trial	(1 trust, 6 lawful access)
1c rule of law	(1 trust, 6 lawful access)
1d economic development	1 trust, 2 free choice, 3 market-driven, 4 standards, 7 liability
2a workability	(3 market-driven, 4 standards, 7 liability)
2b international	8 international cooperation
2c technological sustainability	(3 market-driven, 4 standards)

**6.3. Outline of the framework**

In the following chapters, I shall describe four optional directions (and one non-direction) for addressing the crypto problem (to call them 'solutions' would be too optimistic).<sup>3</sup> I derive these options from the survey of crypto regulations in Chapter 5, and I present them in their logical order of 'police-friendliness'.

- One can *ban cryptography*. This is really not an option. (Chapter 6½)
- If one cannot prohibit cryptography, the police will want to access the keys that cryptocriminals use. By building in some form of *law-enforcement access to keys* in cryptographic products, the police ensures *beforehand* that they can decipher suspect ciphertexts. (Chapter 7)

---

<sup>3</sup> I presume that cracking crypto, although possible in some cases, is insufficient to deal with the problem in general (see 4.5.3), and hence not an option to consider.

- If it turns out that building in law-enforcement access to keys is not possible, the police will have to get the keys *afterwards*. That is, if they encounter encrypted communications or stored data, they can *demand people to decrypt or to give the key*. (Chapter 8)
- If accessing keys (either beforehand or afterwards) is infeasible, the police really has a problem. They will not be able to read encrypted data. In that case, they will have to look for *alternative investigation measures* which do not depend on data that can be encrypted. (Chapter 9)
- Ultimately, if all optional directions have more negative than positive overall consequences, then one can (consciously) decide to do nothing: the *zero option*. (Chapter 10)

I shall describe the how and why to these options, define pros and cons, and relate them to the principles outlined above. In each chapter, I will define the most viable options within each direction, arguing on the basis of the principles. This will give one or two (locally) optimal options for each direction. For clarity, I will conclude each chapter by crudely simplifying the analysis and presenting a table that illustrates how the options match the principles.

Then, the major work will have to be done in Chapter 11. I will define the relevant representative groups (law-abiding crypto users, businesses, law enforcement, suspects). Then, I will argue for the ordering of the principles as I outlined above. By dropping the veil of ignorance over the representatives, and by taking the perspective of the least-advantaged group, I will compare the options, and see which option arguably best reconciles the interests at stake.