

Chapter 1. Introduction

“No,” Ernie said. “We do speak Guugu Yimidirrh, mate.”

“That’s good.”

“Yes. It is good to have a language. Now listen. I can say” – he spoke some words quickly, a muttered rumbling that sounded like worrojoool gangaral – “and you wouldn’t know.”

As he had spoken, Gladys jerked her head out of her grandson’s hands, and blinked hard, and looked away.

“What wouldn’t I know?”

“I said, ‘Kill that white man,’” Ernie said, looking pleased, “and, see, you didn’t know what I said.”

(Paul Theroux, The Happy Isles of Oceania)

1.1. A problem without a solution

Before I started the research that led to this book, I – like the vast majority of the Dutch – had never heard of cryptography, the digitized and automated sister of secret writing. Then, in March 1994, as I braced myself for the job by hiking the Himalayas, cryptography made headlines for a brief period in Dutch newspapers. A pre-draft law had been concocted in the dark recesses of the Dutch Ministries of Justice and Internal Affairs, which would have effectively outlawed cryptography. Someone envisioning a consequent economic disaster leaked it to the press, and the resulting outcry was heard all over the world, reinforced by the Internet community. Its echoes even reached the dark recesses of the Ministries themselves. This pre-draft law was not a Good Thing, they realized. But how then should they address the rapidly spreading use of encoding programs which protect stored data and communications? After all, knowledgeable criminals would be sure to seize the opportunities offered them by uncrackable codes, and leave wiretapping and searching police empty-handed.

Since early 1994, cryptography has indeed spread widely, spurred by explosive growth of the Internet, electronic banking, and electronic transactions. By mid-1998, it has become a common technology that many people use without knowing (in GSM phones, for instance) and that an increasing, though still rather small, number of people use explicitly (in e-mail, for example, or when ordering books online). Cryptography has proved itself a primary tool in information security. Actually, criminals are also – albeit slowly – discovering the potential of cryptography to elude law-enforcement’s scrutiny (many still rely on more traditional tricks, such as using a bunch of mobile phones with untraceable prepaid cards).

With the increasing need in the information society to employ cryptography on the one hand, and with the increasing concern that criminals can effectively escape justice by using

National studies on the crypto controversy

Australia: the Walsh report was released in early 1997 after considerable pressure from Electronic Frontiers Australia; although several sections were not available for national security concerns, the published part is a thorough, consistent, and broad analysis of the issue in the Australian context [Walsh].

Canada: the Task Force on Electronic Commerce issues a discussion paper *A Cryptography Policy Framework for Electronic Commerce* in February 1998, listing several options to address encryption of stored data, encryption of real-time communications, and export controls [TFEC].

Denmark: one of the earliest national reports to appear, the 1995 collection of articles by the Technology Council, *A Danish crypto policy. How to keep digital information secret?*, aptly termed the issue a Gordian knot that badly needed cutting (without suggesting how) [Stripp]. The more elaborate *Report by the Expert Committee on Cryptography*, released in April 1997, by representatives of seven ministries, recommended not to introduce regulation of cryptography in Denmark; however, having only considered mandatory options, they recommended studying the possibilities and consequences of introducing incentive schemes [ECC]. As a result, the Expert Committee continued its work, and in June 1998 released a report recommending – for the time being – not to limit crypto use by incentive schemes either, but to continue to monitor international developments [Fsk].

Sweden: the October 1997 report from the Cabinet Office Reference Group for Cryptographic Issues, *Crypto Policy: Possible Courses of Action for Sweden*, is a broad inventory of digital signature and encryption issues; it recommends free use of cryptography, but is rather optimistic (or pessimistic, depending on your point of view) on the option of voluntary deposit of crypto keys (cf. Chapter 7), apparently assuming that many countries are considering such schemes [Cabinet].

United States: the 1994 Association for Computing Machinery's *Codes, Keys, and Conflicts, Issues in U.S. Crypto Policy* was the first major study of the issue to appear; it is still a valuable analysis of the issues at stake [ACM]. In 1996, the National Research Council, with government, business, and academic members, published its visionarily titled 'Cryptography's Role In Securing the Information Society' (mark the acronym). The extensive and in-depth analysis of all aspects of the crypto conflict and its many informative appendices make it the best report available. The report contains several partial recommendations, among others, not to bar domestic manufacture or use of encryption, and to progressively relax (but not abolish) export controls. [NRC]

cryptography on the other, the *crypto controversy* has emerged as a major problem for governments: how should they balance the conflicting interests of privacy and information security on the one hand with the interests of law enforcement and national security on the other?

Thus, the crypto controversy has become one of the major policy debates of the information society. There are lively discussions on the Internet (special mailing lists have been set up to discuss the issue, such as 'ukcrypto' and the German 'krypto', while other mailing lists and news groups have discussed it extensively, e.g., cypherpunks, cryptography@c2.net, talk.politics.crypto, and sci.crypt). In the parliaments (notably in the US and Germany), and increasingly in national newspapers, the debate is continuing in wider public circles. These discussions show the fairly broad interest in the topic, as well as the extreme positions some lobby groups take in this debate. Often, the discussion has not led the two lobbies of the privacy community ("no regulation whatsoever!") on the one hand and the law-enforcement community ("give us the keys!") on the other to come any closer. Rather, most have repeated well-known arguments and insisted upon their own conclusion being the right one to balance the conflicting interests. The 'middle way' everyone is looking for keeps disappearing across the horizon.

The Dutch government has racked its brains on how to balance the conflicting interests of cybersecurity and cryptocriminals. Tentative suggestions for (partial) solutions are still being discussed. Indeed, many countries have assigned study groups to develop a discussion or position paper on the issue (see sidebar). The most notable of these are the Australian Walsh report and the US NRC report.

If there is one thing these reports have in common, it is that they acknowledge the complexity and importance of the problem while not really knowing how to solve it. I share this common denominator: one thing I will not do in this book is give *the* solution to *the* problem. Instead, I will present a dynamic approach which indicates in what way governments, and in particular the Dutch government, could and should address the problem.

Instead of ‘solutions to the crypto problem’, I will talk of ‘ways to address the crypto problem’. For lack of a simpler term, I will refer to these ways as ‘optional directions’. This indicates that, if one is to resolve the problem, one can look in several directions which may at least provide a way to live with the problem, even if none of them truly solves it.

1.2. What this book is not about

This book is not about *national security and intelligence*. National security agencies have the same problems as law enforcement if their objects of surveillance use cryptography.¹ However, their methods of surveillance, although perhaps the same in practice, differ from those of law enforcement in that, at least in the Netherlands, they are supervised through political procedures, not by legal authorities according to legal procedures. Their use is obscure, as is their effect. Criminal investigation, on the other hand, is, in principle,² subject to court scrutiny, which results in more public data on the use and effectiveness of the investigation measures. I have therefore confined myself in this book to looking at the problems that *law enforcement* faces in the *investigation of crimes*. Although this means that the analysis covers only part of the problem that governments have to address (nefarious use of cryptography), it is – I believe increasingly – felt to be the more important and more urgent part of the problem. Until the mid-1990s, the crypto debate centered for a large part around national security and intelligence, but over the last three years, the debate has gradually shifted towards law-enforcement interests.

This book is not about *export controls*. As a consequence of leaving aside national security problems, I disregard the debate about crypto export controls. These are, after all, targeted at keeping uncrackable cryptography out of the hands of foreign crooks and terrorists – potential objects of intelligence surveillance, but not of law enforcement. Export controls do not see to domestic use of cryptography by criminals (although they may have served in the US as a domestic policy instrument, cf. 5.1.2). A large part of the crypto debate in the United States has revolved around the export controls, but since a few years, it also focuses

1 A nice example of cryptography’s use in a plot threatening national security is provided by Mary, Queen of Scots. As Babington, a former page of Mary’s, conspired to kill Queen Elizabeth of England, he needed the approval of Mary, who was then held under house arrest. The correspondence between them, faithfully encrypted with nomenclators, was exchanged through a double-agent, who forwarded all letters to England’s state cryptanalyst, Phelippes. Once Mary had written an incriminating message, approving of the assassination plot, her fate was sealed, and she was executed shortly afterwards. [Kahn, 121-124]

2 The qualification is needed after IRT-gate, in which InterRegional Teams investigating serious crime turned out to have bypassed court scrutiny to a degree unheard of in Dutch society.

on domestic regulations, following the Clipper fiasco and the SAFE coup in Congress (see 5.3.8). In the Netherlands, domestic controls have always been the focus of the crypto controversy.

This book is also not about *tapping*. Although wiretapping is an important subject in this book – much of the crypto debate discusses safeguarding the future of wiretapping – it is subordinate to the crypto problem. That is, I take as a starting point that wiretapping is allowed under certain conditions, and that the law requires telecom providers to make their networks tappable (see 4.3.1) and to facilitate specific wiretaps. Wiretapping as such is not questioned. Note that in considerable parts of the crypto debate, particularly in the US, and also in the UK, this starting point has itself been challenged: in many discussions, opponents of crypto regulations have argued against wiretapping capabilities as such rather than against regulating cryptography for wiretapping's sake.³ As a consequence of not discussing wiretapping as such, I will not analyze to what extent wiretapping is technically feasible regardless of cryptography. The development of the information and communications infrastructure is posing several technical problems to wiretapping; despite the ardent wish of the legislature to maintain the technical capacity to wiretap, these technical problems may turn out to be a significant obstacle for continuing current-level wiretapping. This is outside the scope of this book. I shall assume here that wiretapping is technically possible, in order to analyze the problems of crypto use for wiretapping. (Note that if the emerging communications infrastructure will turn out to make wiretapping technically difficult as such, the analysis of the crypto problem will have to be reassessed.)

Finally, this book is not about *digital signatures*. A large (and probably the most important) part of the information-security need of the information society concerns the authenticity and integrity of communications and transactions. Digital signatures can fulfill these objectives, and cryptography is a key technology for digital signatures. Policies and (probably) legislation to facilitate the use of digital signatures are called for, and so, a considerable part of the overall crypto policy debate should address this need. Digital signatures as such do not, however, pose a problem for law enforcement. Therefore, I will only deal with digital signatures when this touches upon the law-enforcement problem, notably in section 7.3 when discussing technologies that separate authentication-only from confidentiality cryptography.

1.3. What this book is about

This book is about the law-enforcement concern with cryptocriminals. The central question I answer in this book is:

3 See, for instance, the summary of responses to the 1997 UK consultation document on crypto policy: the “issue of access to keys for law enforcement purposes attracted by far the most comment – particularly from individuals. Much of it was fundamentally opposed to the whole concept of lawful access, and either explicitly or implicitly also rejected the existing powers for lawful access to traffic under the Interception of Communications Act”. [Roche]

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?

1.3.1. Focus on the Netherlands

In a globalized and networked society, one should not look for national solutions to international problems in the field of information and communication technologies (ICT). The information society is global by nature. Moreover, crime, especially organized crime, is increasingly crossing borders and forcing law enforcement to cooperate internationally. Both developments suggest that to address the crypto conflict, one should choose an option which is valid throughout the information society.

I will not do so. Given the complexity and precarious nature of the issue, addressing the problem from the perspective of a single state is difficult; addressing it from an international perspective is impossible. An option has to acknowledge national concerns, legal cultures, the specifics of constitutional protection. It is unrealistic to choose international or even supranational options to address the crypto conflict. The failing effort of the OECD to achieve just that, an international direction of crypto policies, underlines this. The OECD 'guidelines', after all, do not guide. They leave it to every single state to strike a balance somewhere; virtually any balance, packed in proper rhetorics, will satisfy the OECD principles. A compromise between cybersecurity and law-enforcement interests cannot apparently itself be compromised on an international level. States, then, must do it themselves.

This effectively leaves the crypto conflict at a dead end. While national options are not appropriate, international options are not viable. The only way out seems to me to focus on nationally-based options that take the international context as one of their preconditions. I shall look for options that can be implemented in the Netherlands, whether or not other countries implement similar or contrary policies. This, of course, is a major constraint, but it is an inevitable one.

Analyzing the crypto conflict from a Dutch perspective has several advantages. I can give a more detailed and in-depth description of the context in which the problem should be seen, and I can better argue whether particular options fit the legal system and legal culture. Moreover, the Netherlands is a particularly interesting case given 'IRT-gate': the practice of some investigation agencies (IRTs) exploring and increasingly crossing the legal margins of investigation powers. When things had really gotten out of hand, by 1993, a parliamentary inquest had to set things straight and bring Dutch justice back to order. The report of the inquest, usually referred to after its chairman as the Van Traa report, provoked a rethinking of criminal investigation and led to several legislature proposals on investigation measures. This rethinking of investigation law and practice is a felicitous context for the crypto debate, as this is closely linked to one of the central needs of criminal investigation: gathering information.

The national focus does not mean that this book is of interest to Dutch readers only. On the contrary, much of the material covered is equally valid for other countries – it is the details that vary, not the outline. I sometimes illustrate this variation for other countries in sidebars and sections, in order to provide a wider context for the analysis; this is illustrative

A wide gap

The crypto debate features two sides with opposing interests. The privacy lobby and the law-enforcement lobby have discussed the issue extensively, but they do not seem to have come much closer to each other.

Alan McDonald, senior counsel with the FBI, has said that "privacy activists had fought any balance in proposed encryption legislation." He called the extreme privacy positions "ultimately elitist and nondemocratic in that they presumed the views of a knowing privacy cognoscenti should pre-empt the views of the nation's elected officials and the Supreme Court" [quoted in Braun].

Two of the constraints that Mike Nelson formulated for finding an encryption policy that makes everyone happy (or equally unhappy) [Nelson] are particularly telling in this respect:

- Any solution the U.S. government endorses is immediately suspect.
- No one trusts anyone.

On the other side of the debate stands the FBI, as described by Stewart Baker: "the FBI is not too troubled by the bad press it's getting over encryption, or by the privacy and industry complaints – or even by the Congressional harrumphing. (...) in the end, the Bureau believes that Congress will have to mandate crypto controls just as it had to mandate wiretap requirements." [Baker 98a]

rather than systematic. In particular, I often indicate the situation in the US – not to provide a final analysis of the US conflict, but to show the ingredients one can use to transpose my analysis of the Netherlands to the US.

Moreover, one of my major concerns in this book is the methodological issue of how to balance conflicting interests. I value not so much the outcome of this procedure (the particular balance I propose for the Netherlands), but the procedure itself. For other countries, filling in the particulars will vary, but the

procedure I follow to reach an outcome can, I suggest, be equally valuable in other Western countries (and, who knows, in South American countries and South-East Asian (former) tigers).

1.3.2. Outline

The first part of this book defines the context of the crypto conflict. Chapter 2 features the information society and its need for information security. Here, I am lavish with quotes from government policy documents on the importance of information security, in order to provide a counter-weight to the bold law-enforcement statements that will follow later. In Chapter 3, I argue that cryptography is a key technology to provide information security. After a primer on cryptography, I illustrate the importance of encryption by listing many applications, including its benefits for governments themselves. Chapter 4 provides the context of investigation, focusing on the kinds of criminals at issue and their information-management practices, the investigation measures hampered by cryptocriminals, an assessment of the cracking opportunities for the police, and a guesstimate to what extent crypto has obstructed law enforcement to date. In Chapter 5, I survey what laws and regulations have been enacted or planned to deal with the issue. Together, these chapters define the problem and the context in which options will have to be found.

Part II provides a framework to address the crypto conflict. Chapter 6 defines the principles which will guide the procedure of balancing interests. These principles are applied in Chapters 6½-10 to the four directions that options can be looked for (and to one non-direction: banning cryptography or mandating law-enforcement access to keys, Chapter 6½):

- voluntary crypto systems which provide law-enforcement access to keys, including non-confidentiality systems, key escrow, and key recovery (Chapter 7);

- requiring people to provide decryption; the central issues here are to what extent the privilege against self-incrimination and the presumption of innocence allow suspects to be ordered to decrypt, and how such a decryption command can be enforced (Chapter 8);
- alternative investigation measures. Conceptually, once law enforcement cannot access keys or plaintext if the options of accessing keys beforehand (Chapter 7) or afterwards (Chapter 8) do not work, they will have to leave the encrypted data aside and find other ways to gather information. Chapter 9 describes (not exhaustively) possible alternatives to wiretaps and computer searches: direct eavesdropping, intercepting electromagnetic radiation, infiltration, crown witnesses, and data mining;
- doing nothing, which is the only logical thing to do if all possible alternatives turn out to have more negative than positive effects; note that doing nothing is a conscious decision in this respect (Chapter 10).

Chapter 11, finally, is the synthesis of the previous chapters. Taking as input the principles from Chapter 6 and the viable options that emerge from Chapters 7-10, I provide a procedure to address the crypto conflict, inspired by John Rawls' theory of justice. The major interested parties (except the criminals, of course) will match the various options with the principles at stake, and decide which (partial) option or options best balance the conflicting interests in the Dutch context.

The analysis in this book is, in principle, a conceptual one. This does not mean that I disregard details or the way things work out in practice; rather, I have tried to provide an overall, abstracted analysis of the issues at stake. More detailed descriptions of options serve as illustrations and show the pros and cons of the options. The descriptions are far from exhaustive, and often (notably in Chapters 7 and 9), I have chosen a sample of options which may have left other, equally valid, examples unmentioned. Also, in arguing over the real value of a particular option, I have tried to keep reality in mind and not lose myself in long arguments over counter-examples. Particularly, cryptographers excel at inventing ways to subvert solutions and to offer patches for the gaps, inviting others to attack the patches and offer patches for bugs in the patches, and so on ad libitum. With the second round of counter-counterattacks, the debate has often moved far beyond a realistic assessment of real-world issues (which is not to say that these theoretical discussions are not useful). I have also abstracted from particular implementations, should one or the other option be chosen, with respect to the specific legal constraints under which the option could or should be implemented. I assume that the usual legal safeguards apply, such as proper warrants and the principles of subsidiarity and proportionality for investigation powers.

1.3.3. Aim

My overall aim with this book is to provide a conceptual analysis of the crypto problem for law enforcement. I analyze the issues at stake and the pros and cons of the various options to address the problem. By giving a broad overview of the many sides of the problem and of the many valid (and occasionally invalid) arguments, I hope to clarify the debate, to show the nature of the problem (a conflict of interests), and to show how it can be addressed (justifying the choice of particular options by open and argued reasoning in an explicit procedure).

Indeed, the issue of *how* to balance conflicting interests is central to the framework I choose. All too often, people list options and criteria, and jump to the conclusion that one or other option best balances the interests, essentially leaving hidden the process of arriving at this conclusion. A second aim of this book, then, is to bring to light the methodological issue of how to balance interests; I shall do this mainly by making explicit the assumptions I make and by clearly describing the procedure of choosing an option.

Through the conceptual analysis of the problem, I hope this book will help to bridge the gap, still particularly wide in this debate, between technology and law, between cryptographers and lawyers, between privacy activists and governments. Underlying this book is the sense that the two research fields, ICT and law, cannot do without each other. Each has to understand what the other area is about, how it functions, and – perhaps most importantly – how people reason in the other field. Although the crypto problem is essentially a legal problem, addressing it requires knowledge of the technology involved. Moreover, if the resulting policy is to bridge the gap between the two fields, the reasoning must be consistent with the accepted practices of both technology and law. Therefore, the thrust of the argument in this book should be acceptable to specialists in both fields. I have refrained from giving detailed legal or cryptographic analyses and focused instead on combining the two fields in a readable book. If I have succeeded in making the two parties that have so often taken sides against each other in the crypto debate gain some understanding of the other side of the debate, it is sufficient justification for this book.

1.4. How to read this book

I have tried throughout this book to make it readable for everyone interested in the subject, be they lawyers, ICT specialists, cryptographers, cypherpunks, e-merchants, or interested information citizens. I explain terminology and introduce basic concepts of both ICT and law, assuming only a basic knowledge of computers and the Internet. An extensive glossary and abbreviation list of technical and legal terms should help the reader in understanding the text. This does not mean it is always easy to follow (lawyers may require considerable effort to grasp Chapters 3 and 7, whereas ICT specialists may need time for the subtleties of Chapters 4 and 8), but everyone willing to invest time and brain activity should be able to read the book throughout.

Readers can, in principle, skip certain chapters if they wish. For instance, cryptographers will be familiar with most of Chapter 3, and frequent visitors of my online Crypto Law

Survey need not read Chapter 5. Those well-versed in the crypto debate may skim through Part I to see which areas I cover, and move on to Part II. However, readers must bear in mind that the reasoning in Part II is based on the entire context outlined in Part I, and that I do not always explicitly refer back to assumptions and distinctions I have made earlier.

I have tried to make this a reader-friendly book, with illustrations, quotations, and sidebars enlivening the text. The contents of the sidebars and footnotes are usually not essential to the argument, but should not be regarded as less important than the main text⁴ (one of the (few) nice achievements of postmodernism is the blurring of center and margin). Where it does not affect the thrust of the argument, I have occasionally valued readability and understandability over (technical or legal) correctness.

In cryptographic literature, the technology is commonly illustrated by crypto characters Alice and Bob, the friendly personifications of the blank A and B so often encountered in technical texts. I have taken the liberty of extending the crypto family with a few law-enforcement characters, which seemed a good way of illustrating the various options at work.

I use American English, with two exceptions: I Do Not Capitalize Titles, and I use the more consistent British way of indicating dates (dd Month yyyy). All translations are mine.

I use references only to substantiate the text, not to suggest further reading. The references are indicated in the text with square brackets [Fokke & Sukke] and can be found in the bibliography, except the references to newspapers and magazines, which are in italics [*China Daily*, 29 October 1997]. Where useful, I refer to page numbers [Rawls, 121], partly to facilitate looking up the reference, and partly out of nostalgia that there are still page numbers to refer to. With longer electronic documents, I refer to sections [Walsh, 3.2.1]. Dutch legislation proposals are referred to as [25880, nrs 1-2, 197]: parliamentary document series 25880 (*Legislation for the electronic highway*, the title is mentioned in the bibliography), numbers 1-2, page 197. EU and EC documents are referred to by their number [COM(94) 347, 96/C329/01]. These are separately referenced in the bibliography. Case law is referred to by the Court name (e.g., HR = Dutch Supreme Court) and date or (mostly with European and US cases) by their (nick)name; the full references can be found in the case-law section of the bibliography.

The research of this book was finalized on 1 July 1998. Later developments that are important to the overall reasoning of this book (notably, enacting of legislation that is still at the drafting stage when this book goes to print), I will update on my homepage <<http://cwis.kub.nl/~frw/people/koops/thesis/update.htm>>.

4 Cf. Anthony Grafton, *The footnote. A curious history*, London: Faber and Faber, 1997.