

# The crypto controversy

## A key conflict in the information society

Bert-Jaap Koops  
Tilburg University  
Eindhoven University of Technology

KLUWER LAW INTERNATIONAL  
The Hague / London / Boston

Law and Electronic Commerce Volume 6

ISBN 90-411-1143-3

All rights reserved.

© 1999 Bert-Jaap Koops

Published by Kluwer Law International  
P.O. Box 85889  
2508 CN The Hague, The Netherlands

Sold and distributed by Kluwer Law International  
675 Massachusetts Avenue, Cambridge, MA 02139, U.S.A.  
P.O. Box 322, 3300 AH Dordrecht, The Netherlands

*Only connect...*

*(E.M. Forster)*



# Table of contents

Acknowledgements .....	xv
Chapter 1. Introduction .....	1
1.1. A problem without a solution .....	1
<i>National studies on the crypto controversy (2)</i>	
1.2. What this book is not about .....	3
1.3. What this book is about .....	4
1.3.1. Focus on the Netherlands .....	5
<i>A wide gap (6)</i>	
1.3.2. Outline .....	6
1.3.3. Aim .....	7
1.4. How to read this book .....	8
 <b>Part I. Problem and context</b>	
Chapter 2. An information society needs information security .....	13
2.1. The information society .....	13
2.1.1. Developments .....	13
2.1.2. Information society policy .....	15
United States .....	15
European Union .....	16
The Netherlands .....	17
2.1.3. Building blocks and participants .....	19
2.1.4. Problems .....	20
<i>The Internet (22)</i>	
2.2. Information security .....	23
2.2.1. Objectives .....	24
2.2.2. Threats .....	24
<i>Political viruses (25)</i>	
2.2.3. Measures .....	26
<i>Information-security policy (27)</i>	
2.2.4. Governments' role in information security .....	27
2.2.5. Information security in Dutch government .....	28
<i>Information security in EU and Dutch law (29)</i>	
2.3. Conclusion .....	31
Chapter 3. Cryptography, a key technology for information security .....	33
3.1. Cryptography .....	34
3.1.1. History .....	34
<i>Atbash (34)</i>	
<i>Terminology (35)</i>	
3.1.2. Intermezzo – dramatis personae .....	35
3.1.3. Symmetric and public-key cryptography .....	35
The working of public-key cryptography .....	37
Authenticity, integrity, and non-repudiation .....	38

3.1.4. Cryptanalysis and the strength of crypto systems	40
<i>Distributed attacks (42)</i>	
3.1.5. Key length	42
<i>Developments that may shake the field (43)</i>	
3.1.6. Key management	43
3.1.7. More distinctions	45
3.1.8. Hiding cryptography	46
Detecting cryptography	47
3.1.9. Protocols	48
3.2. Applications	48
3.2.1. Providers	48
3.2.2. Government	51
3.2.3. Other users	52
Financial applications	52
Privacy and sensitive data	53
Human rights	54
Public and private networks	55
Other applications	56
3.2.4. Cryptography in practice	57
3.3. Conclusion – the importance of cryptography	57
Chapter 4. Cryptocriminals, a public concern	59
4.1. The crime society	60
4.1.1. Organized crime	60
Activities	61
Seriousness	62
Information behavior	62
Use of cryptography	64
4.1.2. Business crime	65
Seriousness	65
Information behavior and use of cryptography	66
4.1.3. Computer crime	66
Seriousness	67
Information behavior and use of cryptography	68
4.1.4. Other types of serious crime	68
4.2. Investigation	69
4.2.1. Developments in criminal investigation	69
<i>IRT-gate (71)</i>	
<i>Draft legislation (72)</i>	
4.2.2. The organization of criminal investigation	73
4.2.3. The stages of criminal investigation	74
4.3. Gathering data in transport	75
4.3.1. Tapping	76
Conditions	76
<i>The effectiveness of tapping (78)</i>	
Legal problems	78
Technical problems	79
Maintaining tappability	80
4.3.2. Tapping in other countries	81
<i>Echelon (82)</i>	
4.3.3. Traffic analysis	84
4.4. Data storage	85

TABLE OF CONTENTS

xi

4.4.1. Handing over data	85
<i>Criminal financial inquest (85)</i>	
4.4.2. Search and seizure	86
<i>International investigation (87)</i>	
4.4.3. Searching elsewhere	87
4.4.4. Providing access	88
4.5. Problems through encryption	88
4.5.1. Main crypto-problems	89
4.5.2. Cryptocriminals in practice	90
4.5.3. Cracking evidence	91
4.5.4. Further crypto-problems	93
<i>Problems in proof (93)</i>	
4.5.5. Scope of the problem	95
4.6. Conclusion	95
<i>The main crypto problems for law enforcement (96)</i>	
Chapter 5. A survey of cryptography laws and regulations	97
5.1. Export and import controls	97
5.1.1. COCOM and Wassenaar Arrangement	97
5.1.2. United States	98
5.1.3. Import restrictions	99
5.2. International developments	99
5.2.1. OECD	99
<i>Terminology (101)</i>	
5.2.2. European Union	101
5.2.3. Other European initiatives	102
5.3. Domestic crypto laws per country	103
5.3.1. Belgium	103
5.3.2. Denmark	103
5.3.3. France	104
5.3.4. Germany	105
5.3.5. The Netherlands	106
5.3.6. Russian Federation	107
5.3.7. United Kingdom	107
5.3.8. United States of America	109
Escrowed Encryption Standard (Clipper)	109
Key Management Infrastructure	110
NRC report	110
Broad Encryption Policy	110
Draft key-recovery legislation	111
Congress bills	111
Conclusion	112
5.4. Concluding remarks	112
<b>Part II. Framework and analysis</b>	
Chapter 6. Framework and set of principles	117
6.1. Choosing a framework	118
6.2. A set of principles	119
6.2.1. Fundamental principles	119
6.2.2. Less fundamental principles	121

	<i>Comparison with the OECD principles (123)</i>	
6.3.	Outline of the framework	123
Chapter 6½.	Outlawing cryptography	125
6½.1.	A crypto ban does not help the police	126
	<i>What is a plain text? (128)</i>	
	<i>Mandatory LEAK and constitutional rights (129)</i>	
6½.2.	A crypto ban does hamper good guys	130
6½.3.	Conclusion	131
Chapter 7.	LEAKing through the Public Key Infrastructure	133
7.1.	Public Key Infrastructures	134
	<i>Terminology (135)</i>	
	<i>The crypto family revisited (137)</i>	
7.2.	Public Key Infrastructures and LEAK	138
7.3.	Non-confidentiality cryptography	139
7.3.1.	Working of DSA	140
7.3.2.	Subversive use of DSA	140
7.3.3.	Assessment of DSA	141
7.4.	LEAKing through key deposits	143
7.4.1.	LEAK techniques	143
7.4.2.	Escrowed Encryption Initiative	144
	Defeating the LEAF	146
	Software key escrow	147
	<i>Temptations for Polly (148)</i>	
7.4.3.	Royal Holloway's international TTP scheme	148
7.4.4.	Add-ons	151
	Splitting keys	151
	Traceable ciphertexts	152
	<i>Cryptographic warrant bounds and edge surveillance (153)</i>	
7.5.	LEAKing through key recovery	153
7.5.1.	Commercial Key Escrow	154
	<i>Translucent cryptography (154)</i>	
7.5.2.	PGP's Corporate Message Recovery	155
7.5.3.	International Cryptography Framework	156
7.5.4.	Key Recovery Alliance	156
7.6.	LEAKy issues	157
	<i>Abuse by government (158)</i>	
7.7.	Assessing the LEAK options	159
7.7.1.	Effectiveness of LEAK systems	159
7.7.2.	The options	162
7.7.3.	Applying the criteria	162
7.7.4.	Conclusion	165
Chapter 8.	Demanding decryption	167
8.1.	Preliminary distinctions	168
8.1.1.	Demanding decryption or key delivery?	168
8.1.2.	Decrypting stored and communicated ciphertexts	169
8.2.	Demanding non-suspects to decrypt	170
8.3.	Demanding suspect corporations to decrypt	172
8.4.	Demanding individual suspects to decrypt	174
8.5.	The rationale behind the privilege against self-incrimination	177

8.6. Is it possible to create a law demanding decryption? .....	180
<i>Voices for demanding decryption (181)</i>	
8.7. How to enforce a decryption command .....	182
8.7.1. Penalize a refusal to cooperate .....	182
8.7.2. Penalize cryptocriminal use .....	186
8.7.3. Reverse the burden of proof .....	189
<i>Local precedents for reversing the burden of proof (190)</i>	
8.8. Assessing the decryption command .....	194
8.8.1. The decryption command in current law .....	194
8.8.2. Options for enforcing a decryption command .....	195
8.8.3. Applying the criteria .....	196
8.8.4. Conclusion .....	200
Chapter 9. Alternative investigation measures .....	203
9.1. 'Direct eavesdropping' .....	204
9.1.1. Description .....	205
9.1.2. Situations, crimes, and encryption .....	206
9.1.3. Legal status in the Netherlands .....	207
9.1.4. Situation in other countries .....	209
9.1.5. Conclusion .....	210
9.2. Tempest monitoring .....	211
9.2.1. Description .....	211
9.2.2. Situations, crimes, and encryption .....	213
9.2.3. Legal status in the Netherlands .....	213
9.2.4. Situation in other countries .....	214
9.2.5. Conclusion .....	215
9.3. Infiltration .....	215
9.3.1. Description .....	215
9.3.2. Situations, crimes, and encryption .....	217
9.3.3. Legal status in the Netherlands .....	218
9.3.4. Situation in other countries .....	219
9.3.5. Conclusion .....	219
9.4. Crown witnesses .....	220
9.4.1. Description .....	220
9.4.2. Situations, crimes, and encryption .....	222
9.4.3. Legal status in the Netherlands .....	222
9.4.4. Situation in other countries .....	223
9.4.5. Conclusion .....	224
9.5. Data mining .....	224
9.5.1. Description .....	224
9.5.2. Situations, crimes, and encryption .....	225
9.5.3. Legal status in the Netherlands .....	226
9.5.4. Conclusion .....	227
9.6. Assessing the alternative investigation measures .....	227
9.6.1. The options of alternative investigation measures .....	227
9.6.2. Applying the criteria .....	229
9.6.3. Conclusion .....	232
Chapter 10. The zero option .....	233
10.1. The zero option .....	233
10.2. Applying the criteria .....	235
10.3. Conclusion .....	236

Chapter 11. Reconciling interests .....	237
11.1. Rawls and social justice .....	238
11.2. The crypto conflict and criminal justice .....	240
11.3. Description of the problem .....	241
11.3.1. The original position .....	241
11.3.2. Representative groups and their veil of ignorance .....	242
11.4. The crypto policy conference .....	243
11.4.1. The least advantaged group .....	243
11.4.2. Principles and ordering rules .....	244
11.4.3. Selecting the options .....	245
11.4.4. Narrowing down the problem .....	252
11.4.5. The key decision .....	252
11.4.6. Looking at the future .....	255
11.4.7. Evaluation .....	257
11.5. Agenda for a US conference .....	257
11.6. Conclusion .....	259
Summary .....	261
Abbreviations .....	267
Glossary .....	269
Glossary of terms .....	269
Glossary of legal terms (English-Dutch) .....	271
Glossary of laws and regulations (English-Dutch) .....	271
Glossary of organizations (English-Dutch) .....	271
Bibliography .....	273
Legislative proposals, decisions, and other parliamentary documents .....	283
Dutch .....	283
European .....	283
Case Law .....	284
Dutch .....	284
European .....	285
US .....	285
About the author .....	287
Samenvatting .....	289

## Acknowledgements

*This book is the result of a Ph.D. research project financed by the Co-operation Centre Tilburg and Eindhoven Universities. I am grateful for their support. The staff of the Co-operation Centre, in particular Karen Leurs, Els van Loon, and Marianne Wagemans, have been helpful in providing excellent working conditions.*

*My supervisors have supported and stimulated me from the start. Marc Groenhuijsen has been the best supervisor I could have wished, stimulating and valuing my work, and carefully correcting what errors I was apt to make. Our discussions were without exception inspiring and thought-provoking. Jan Smits is a living example of the integration of IT and law, and he has transferred his fascination for this research field to me in many discussions, which were all the more relevant and agreeable for not always being to the point. Henk van Tilborg improved my knowledge of cryptography and provided helpful feedback on the technological sections of this book. Paul Wiemans, the instigator of the project, has cheerfully guided me into the research topic as well as into the university, and his careful analysis of legal issues has several times provoked me to reconsider an immature conclusion. Finally, Corien Prins, as head of the IT-law section of the Tilburg University law faculty, created an inspiring environment for research, and her judicious proofreading of the book helped me to improve it in various ways. To all, I am grateful for their support, for their inspiration, and for their confidence in my individual way of working.*

*Several people have commented on parts of this book. Thanks are due to Wibren van der Burg, Petrus van Duyne, Simone van der Hof, Bert Kroese, Elisabetta Manunza, Christian Meyn, Bart Streumer, Anton Vedder, and Eric Verheul for offering their expertise on particular subjects in criticizing relevant chapters. Besides, Eric Verheul has helped me gain a better knowledge of applied cryptography, and our joint work on an article proved beneficial to this book as well. I have had helpful discussions with Henk Algra, Ronald de Bruin, Hans Henselaar, Cees Jansen, Jan Koers, Dick Komen, Ronald Prins, and Henk van Rossum on the larger issues of this research. Marianne Sanders proved an excellent as well as entertaining teacher who gave me the courage and tools to write this book in English. I thank Jean-Marc van Tol, Bastiaan Geleijnse, and John Reid for their illustrations, and I hope this book may help Fokke and Sukke to travel abroad more frequently.*

*I also thank the many people I met on the electronic highway, in particular all those who provided information for my online Crypto Law Survey. The people discussing on several mailing lists, notably on cypherpunks, Perry's cryptography, ukcrypto, and krypto, helped me to gain an understanding of a wide range of issues related to my research, and – even with their occasionally less ideal signal-to-noise ratios – they have been a wonderful source of information.*

*Quite less virtual but equally stimulating have been my colleagues, in particular of the penal-law department and the IT-law section of Tilburg University, and of the law and technology section of Eindhoven University of Technology. The secretaries, especially Vivian Carter, Marian de Jong, and Paula Verheij, have also helped to make my work agreeable and efficient. Finally, I thank Karin van Tuijn, my invaluable room mate of early days, for our discussions on numerous vital and trivial subjects.*

*I am grateful to my parents for their continuous support of my personal development, my studies, and my other activities. This book is the result of the combination of all these, and my parents deserve credit for at least the good parts of this book. Last and foremost, Ad van der Meer has supported me in more ways than I can express gratitude for. Throughout this research project, he has been the most scrupulous proofreader of my writings, and he has made my life a happy one. I will only be able to return all he has done for me once he starts writing his Ph.D. thesis.*

*Bert-Jaap Koops  
August 1998*