

BUILDING IN BIG BROTHER

The Cryptographic Policy Debate

Edited by

Lance J. Hoffman

*Institute for Computer and Telecommunications Systems Policy and
Department of Electrical Engineering and Computer Science
School of Engineering and Applied Science
The George Washington University*



Springer

Contents

Preface *vii*
Contributors *xv*
Introduction *I*

PART I Background

CHAPTER 1 *Cryptography (From Julius Caesar through Public Key Cryptosystems): Methods to Keep Secrets Secret* 7

1 Encryption *10*
Deborah Russell and G. T. Gangemi, Sr.

2 Data Encryption Devices: Overview Technology Analysis *24*
Rebecca J. Duncan, Datapro Information Services Group

3 Answers to Frequently Asked Questions about Today's Cryptography *33*
RSA Laboratories

4 Cryptography in Public: A Brief History *41*
Association for Computing Machinery, U.S. Public Policy Committee

5 Internet Privacy Enhanced Mail *51*
Stephen T. Kent

6 Privacy in Today's Wireless Environment *76*
Kim Lawson-Jenkins

7 Federal Information Processing Standards Publication 186 (1994 May 19): Specifications for the Digital Signature Standard (DSS) *84*
U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology

8 Federal Information Processing Standards Publication 180 (1993 May 11): Specifications for the Secure Hash Standard (SHS) *87*
U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology

9 Pretty Good Privacy: Public Key Encryption for the Masses *93*
Philip Zimmermann

CHAPTER 2	<i>Key Escrow Cryptosystems: Keeping Secrets Secret Except When...</i>	109
1	The U.S. Key Escrow Encryption Technology <i>Dorothy E. Denning</i>	111
2	SKIPJACK Review: Interim Report <i>Ernest F. Brickell, Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman</i>	119
3	Protocol Failure in the Escrowed Encryption Standard <i>Matt Blaze</i>	131
4	CAPSTONE Chip Technology <i>National Institute of Standards and Technology</i>	147
5	Fair Cryptosystems <i>Silvio Micali</i>	149
6	Software Key Escrow: A Better Solution for Law Enforcement's Needs? <i>Stephen T. Walker</i>	174
7	A New Approach to Software Key Escrow Encryption <i>David M. Balenson, Carl M. Ellison, Steven B. Lipner, Stephen T. Walker</i>	180
8	International Key Escrow Encryption: Proposed Objectives and Options <i>Dorothy E. Denning</i>	208
PART II	Current Government Policy	227
CHAPTER 3	<i>The U.S. Government Policy Solution: Key Escrow Cryptosystems, Policies, Procedures, and Legislation</i>	229
1	Statement of the Press Secretary <i>The White House, Office of the Press Secretary</i>	232
2	Statement of the Vice President <i>The White House, Office of the Vice President</i>	235
3	Vice President's Letter to Representative Maria Cantwell <i>Albert Gore</i>	236

- 4 Encryption—Export Control Reform 239
Martha Harris
- 5 Attorney General Makes Key Escrow Announcements 241
U.S. Department of Justice, Office of the Attorney General
- 6 Authorization Procedures for Release of Encryption Key Components
in Conjunction with Intercepts Pursuant to Title III and FISA 243
U.S. Department of Justice
- 7 Encryption Standards and Procedures Act of 1994 247
*Staff, Committee on Science, Space, and Technology, U.S. House of
Representatives*
- 8 Comments on Encryption Standards and Procedures Act 257
Electronic Privacy Information Center
- CHAPTER 4 *The Policy Debate: How Controlled a Global Information
Infrastructure do We Want, and Who Decides?* 263**
- 1 The Cypherpunks vs. Uncle Sam 266
Steven Levy
- 2 Testimony Before the Subcommittee on Technology, Environment,
and Aviation of the Committee on Science, Space, and Technology of
the U.S. House of Representatives 284
Dorothy E. Denning
- 3 Wiretaps for a Wireless Age 292
David Gelemter
- 4 Don't Worry Be Happy 295
Stewart A. Baker
- 5 So, People, We Have a Fight on Our Hands 302
Bruce Sterling
- 6 Jackboots on the Infobahn 307
John Perry Barlow
- 7 'Secret' Agency Steps Over the Line 316
Washington Technology
- 8 A Closer Look on Wiretapping 318
New York Times Editorial

PART III	Aspects of Cryptographic Policy	321
CHAPTER 5	<i>Law Enforcement: What Does It Cost to Commit a Perfect Crime?</i>	323
	Digital Telephony and Communications Privacy Improvement Act of 1994	325
	<i>103rd Congress, 2nd Session</i>	
	Summary Statement before the Subcommittee on Technology and the Law of the Committee on the Judiciary, United States Senate and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives	343
	<i>Louis J. Freeh</i>	
3	EFF Statement on and Analysis of Digital Telephony Act	354
	<i>Electronic Frontier Foundation</i>	
4	EPIC Statement on Wiretap Bill	362
	<i>Electronic Privacy Information Center</i>	
5	Benefits and Costs of Legislation to Ensure the Government's Continued Capability to Investigate Crime with the Implementation of New Telecommunications Technologies	364
	<i>Department of Justice</i>	
6	Digital Telephony—Cost-Benefit Analysis	385
	<i>Betsy Anderson, Todd Buchholz</i>	
7	Digital Telephony—Cost-Benefit Analysis	387
	<i>David McIntosh, James Gattuso</i>	
8	Digital Telephony—Cost-Benefit Analysis	389
	<i>Ron Levy</i>	
CHAPTER 6	<i>Civil Liberties: Safeguarding Privacy (and More) in a Digital, Tappable Age</i>	391
1	The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology	393
	<i>Whitfield Diffie</i>	
2	Genie Is Out of the Bottle	400
	<i>William M. Bulkeley</i>	
3	DPSWG Letter to President Clinton on Clipper	406
	<i>Digital Privacy and Security Working Group</i>	

4	Cryptographic Issue Statements: Letter to the Computer System Security and Privacy Advisory Board	409
	<i>American Civil Liberties Union</i>	
5	The Constitutionality of Mandatory Key Escrow—A First Look	413
	<i>A. Michael Froomkin</i>	
6	Review and Analysis of U.S. Laws, Regulations, and Case Laws Pertaining to the Use of Commercial Encryption Products for Voice and Data Communications	435
	<i>James Chandler, Diana Arrington, Lamarris Gill, and Donna Berkelhammer</i>	
7	On Blind Signatures and Perfect Crimes	449
	<i>Sebastian von Solms and David Naccache</i>	
CHAPTER 7	Export Policy: Prudent Controls in a Risky World or Making the World Safe for Foreign Competition?	453
1	Encryption's International Labyrinth	456
	<i>David S. Bernstein</i>	
2	Federal Policy Impact on U.S. Corporate Vulnerability to Economic Espionage	460
	<i>Geoffrey W. Turner</i>	
3	Testimony Before the Committee on the Judiciary Subcommittee on Technology and the Law of the United States Senate	477
	<i>Stephen T. Walker</i>	
4	Technology and Software Controls	507
	<i>Larry E. Christensen</i>	
5	State Department Ruling on Cryptographic Export Media	535
	<i>United States Department of State</i>	
6	Constitutionality Under the First Amendment of ITAR Restrictions on Public Cryptography	537
	<i>John M. Harmon</i>	
	Afterword	549
	List of Acronyms	553
	Index	555