



TABLE OF CONTENTS

Acknowledgments v
Introduction 1

PART ONE: GUARDING OUR PRIVACY IN THE INFORMATION AGE:

An Overview of Surveillance 3

- I've Nothing to Hide. Why Do I Need Privacy? 4
- What Price for Your Secrets? 7
- Who Is Leaking Our Secrets? 11
- Privacy Defined 13
- A Few Privacy Controversies 17
- Participants in the Privacy Debate 19
- A "Surveillance Age" 21
- Electronic Surveillance 23
- Optical Surveillance 26
- Managerial Surveillance 27
- Biological Surveillance 30
- Why Privacy is Controversial 32
- How Computers Help Snoops 35
- The Dangers of a Cash-Free Society 38
- The Cash-Free Look 39
 - Cash-free benefits 39
 - Cash-free nightmares 40
- Why Is Big Brother in Kindergarten? 42
- The FBI's Digital Telephony Proposal 45
- Do You Want a National ID? 48
- Why Would You Use an Identity Card? 50
- A Prototypical National ID: Your Social Security
 - Number and How to Protect It 52
- Chris Hibbert of CPSR Speaks Out 53
- Aren't Computer Files and E-Mail Already Safe? 61
- Password Protection: What They Don't Tell You 63
- The Guardians of Cyberspace 64
- Anonymous Remailers 65



PART TWO: CRYPTOLOGY ("CRYPTO"):

Roots of the Clipper Chip Controversy 69

 What Is Cryptology ("Crypto")? 70

 Where to Meet Cryptologists 75

 The Powers and Limitations of Crypto 76

 What Is High-Quality Crypto? 76

 Data Encryption Standard (DES) 78

 What Is RSA? 80

 International Data Encryption Algorithm (IDEA) 83

 Digital Signatures 83

 Popularizing Digital Signatures 85

 What Are DigiCash and Blind Signatures? 87

 Steganography 90

 Hiding in Pictures: Stego 92

 Should Crypto Be Software or Hardware? 94

 Crypto Is a "Munition" and Export Controlled! 96

 What Is the Clipper Initiative? 99

 Crypto Experts Oppose Clipper 102

 White House Press Release on Clipper 106

 CPSR's Clipper Chip Petition 110

 The Association of Computing Machinery Speaks Out 111

 Dr. Matt Blaze Finds Clipper Flaw 114

 Vice-President Gore's Letter to Representative Cantwell 115

 EFF Analysis of Vice-President Gore's Letter 118

 Current Status of the Clipper Initiative 122

 Where Can You Read the Latest Crypto News? 123

PART THREE: PGP: Pretty Good Privacy

125

 What Is PGP? 126

 Who Created PGP? 127

 Philip Zimmermann's Statement to Congress 129

 Who's Using PGP? 135

 How Safe is PGP? Will it Really Protect You? 136

 Does PGP Provide Too Much Privacy? 138

 Which Version of PGP You Should Get 140



MIT PGP Version 2.6 140
ViaCrypt PGP Version 2.7 141
Finding PGP 142
Registering with a Public Key Server 144
Stable Large Email Database (SLED). 146
Support For PGP Data Encryption 147
Privacy Protection and Controlling Your Personal Data 147
For More Information on SLED 148
Finding the Latest PGP News 148

PART FOUR: USING PGP ON THE PC 151

Quick Start For Manual Haters 152
Installing PGP on Your PC. 153
Setting Your Time Zone 156
Escaping Panic If You Get Lost 157
Selecting Which PGP Crypto To Use 157
Using PGP's Conventional Cryptography. 158
Encrypting with Conventional Cryptography 158
Decrypting with Conventional Cryptography 160
Using PGP's Public Key Cryptography 162
Creating and Organizing PGP Keys 162
 Generating your public and secret keys. 162
 Where PGP stores your public and secret keys 166
 Viewing your public key ring 168
 Looking at your public key. 170
 Adding a key to your key ring. 174
 Removing a key or user ID from your key ring 176
 Viewing the "fingerprint" of a public key. 177
 Selecting keys via key ID 178
 Signing a public key 179
 Viewing the signatures on your public key ring. 181
 Removing signatures from a public key. 182
 Checking the certifications on your key ring. 183
 Editing your trust for a user ID. 184
 Editing your user ID or pass phrase 185
 Disabling/re-enabling a key on your public key ring. 187



Creating a key compromise certificate	189
Encrypting with PGP's Public Key Cryptography	191
Encrypting a message to one person	191
Encrypting a message to several people	192
Making an ASCII file for e-mail	193
Encrypting a message for e-mail	194
Adding a comment line to ViaCrypt PGP's output	196
Signing a message with your secret key	197
Encrypt "For Her Eyes Only"	199
Encrypt and wipe textfile	201
Encrypt and convert to local text convention	202
Combining encryption options	203
Decrypting with PGP's Public Key Crypto	203
Basic public key decryption	203
Where to put the decrypted files?	205
Decrypting e-mail	206
Decrypting for your screen only	208
Recovering the original filename	208
Advanced Digital Signatures	209
Clear signing a plaintext message	209
How secure are clear signed messages?	212
Useful batch files	214
Separating signatures from messages	217
Detaching a signature certificate	219
Leaving a signature intact after decryption	220
Setting Configuration Parameters	221
Examining and Editing Your CONFIG.TXT File	221
Adding a Comment Line to ViaCrypt PGP's Output	223
Alternative Locations for Pubring, Secring, or Randseed	223
ARMOR (ASCII Armor Output)	224
ARMORLINES (Size of ASCII Armor Multipart Files)	224
BAKRING (File Name for Backup Secret Keyring)	224
CERT_DEPTH (How Deep May Introducers Be Nested)	225
CHARSET (Local Character Set for Text Files)	225
CLEARSIG (Cleartext Signed Messages)	226



COMPATIBILITY (Of PGP Versions) 226

COMPLETES_NEEDED (Number of Trusted Introducers) 227

COMPRESS (Enable Compression) 227

INTERACTIVE (Ask for Confirmation for Key Adds). 227

KEEPBINARy (Keep Binary Ciphertext Files
After Decrypting) 227

LANGUAGE (Foreign Language Selector) 227

MARGINAL_NEEDED (Number of Marginally
Trusted Introducers Needed) 228

MYNAME (User ID for Making Signatures) 228

SHOWPASS (Echo Pass Phrase to User) 228

TEXTMODE (Assuming Plaintext is a Text File). 228

TMP (Directory Path Name for Temporary Files) 229

VERBOSE (Quiet, Normal, or Verbose Messages) 229

Security Considerations (For Paranoids Only) 229

Has Anyone Tampered with Your PGP? 230

Ensuring That Your Computer Is Virus- and Hacker-Free 230

Are You Telling Your Friends Too Much? 232

Where Are Your "Deleted" Files? 232

Is Anyone Fooling with Your Public Key? 233

Is Someone Listening to Your Keystrokes? 233

Is a Traffic Cop Watching You? 233

Are You on a Party Line? 234

What is the Cost of Paranoia? 234

PART FIVE: Bibliography 235

PART SIX: Appendix

Pro Privacy Cyberspace Resources 243

Computer Professionals for Social Responsibility 244

Electronic Frontier Foundation 247

Electronic Privacy Information Center 253

The Privacy Journal 260

INDEX 275