

A Gift of Fire, 2nd edition (Contents)

Preface	ix
1 Unwrapping the Gift	1
1.1 The Ubiquity of Computers and the Rapid Pace of Change	2
1.2 Examining the Gift: An Introduction to Some Issues and Themes	4
1.2.1 Issues	4
1.2.2 Themes	8
1.3 Appreciating the Benefits	11
1.3.1 The World Wide Web, Games, Crime Fighting, and More	11
1.3.2 Health and Medicine	18
1.3.3 Tools for Disabled People	23
1.3.4 Automation	25
1.3.5 Identification, Sensors, and Tracking Systems	26
1.3.6 Reducing Paper Use and Trash	28
1.3.7 Some Observations	28
2 Privacy and Personal Information	35
2.1 The Impact of Computer Technology	36
2.1.1 Introduction	36
2.1.2 Risks of the Technology	38
2.2 “Big Brother Is Watching You.”	41
2.2.1 Databases	42
2.2.2 The Fourth Amendment and Expectation of Privacy	47
2.2.3 More Search and Surveillance Tools	51
2.3 Consumer Information	54
2.3.1 Databases and Marketing	54
2.3.2 Children on the Web	58
2.3.3 Credit Bureaus	58
2.3.4 Principles for Data Collection and Use	59
2.4 More Privacy Risks	61
2.4.1 Social Security Numbers and National ID Systems	61
2.4.2 Personal Health and Medical Information	64
2.4.3 Public Records: Access vs. Privacy	68
2.5 Protecting Privacy: Education, Technology, and Markets	69
2.5.1 Awareness	69

2.5.2	Privacy Technologies and Market Responses	70
2.6	Protecting Privacy: Law and Regulation	73
2.6.1	Philosophical Views	73
2.6.2	Contrasting Viewpoints	78
2.6.3	Contracts and Regulations	81
3	Encryption and Interception of Communications	96
3.1	Overview of the Controversies	97
3.2	Intercepting Communications	98
3.2.1	Wiretapping	98
3.2.2	Designing Communications Systems for Interception and Tracking	100
3.2.3	Carnivore	104
3.2.4	The National Security Agency and Echelon	106
3.3	Cryptography and Its Uses	109
3.3.1	Cryptography and Public Key Cryptography	109
3.3.2	Uses of Encryption	111
3.3.3	Steganography	115
3.4	Encryption Policy: Access to Software, Keys, and Plaintext	115
3.4.1	Secrecy and Export Controls	115
3.4.2	Domestic Encryption Controls?	120
3.5	Fundamental Issues	125
3.5.1	The Role of Secrecy	125
3.5.2	The Ever-Changing Status Quo	126
3.5.3	Trust in Government	127
4	Can We Trust the Computer?	135
4.1	What Can Go Wrong?	136
4.1.1	Questions About Reliability and Safety	136
4.1.2	Problems for Individuals	138
4.1.3	System Failures	142
4.1.4	Safety-Critical Applications	148
4.2	Case Study: The Therac-25	149
4.2.1	Therac-25 Radiation Overdoses	149
4.2.2	Software and Design Problems	150
4.2.3	Why So Many Incidents?	152
4.2.4	Observations and Perspective	153
4.3	Increasing Reliability and Safety	154
4.3.1	What Goes Wrong?	154
4.3.2	Professional Techniques	157
4.3.3	Law and Regulation	160
4.3.4	Taking Responsibility	164
4.4	Perspectives on Failures, Dependence, Risk, and Progress	165
4.4.1	Putting Failures in Perspective	165
4.4.2	Are We Too Dependent On Computers?	167
4.4.3	Observations	170

4.5	Computer Models	171
4.5.1	Evaluating Models	171
4.5.2	Car Crash-Analysis Programs	174
4.5.3	Climate Models and Global Warming	176
5	Freedom of Speech in Cyberspace	192
5.1	Changing Communications Paradigms	193
5.2	Offensive Speech and Censorship in Cyberspace	197
5.2.1	What Is There? What Is Illegal?	197
5.2.2	Material Inappropriate for Children	199
5.2.3	Censorship Laws	201
5.2.4	Internet Access in Libraries and Schools	203
5.2.5	Talking About Bombs—or Farming	207
5.2.6	Challenging Old Regulatory Paradigms and Special Interests	208
5.2.7	Censorship on the Global Net	209
5.3	Anonymity	212
5.3.1	<i>Common Sense</i> and the Internet	213
5.3.2	Is Anonymity Protected?	214
5.3.3	Against Anonymity	217
5.4	Spam	218
5.4.1	What's the Problem?	218
5.4.2	Cases and Free Speech Issues	219
5.4.3	Solutions	220
5.5	Ensuring Valuable and Diverse Content	223
6	Intellectual Property	234
6.1	Intellectual Property and Changing Technology	235
6.1.1	What Is Intellectual Property?	235
6.1.2	Problems from New Technologies	237
6.2	Copyright Law	239
6.2.1	A Bit of History	239
6.2.2	The Fair-Use Doctrine	241
6.2.3	Fair-Use Cases	242
6.3	Copying Music, Movies, Software, and Books	244
6.3.1	From Floppies to the Web	244
6.3.2	The Napster Case	245
6.3.3	Software Piracy	249
6.3.4	Ethical Arguments About Copying	252
6.4	Solutions (Good and Bad)	254
6.4.1	Technology, Markets, and Law	254
6.4.2	Restrictions and Bans on Technology	259
6.4.3	The Future of Copyright	263
6.5	Free-Speech Issues	264
6.6	Free Software	266
6.6.1	What Is Free Software?	266

6.6.2	Should All Software Be Free?	267
6.7	Issues for Software Developers	269
6.7.1	Copyright or Patent?	269
6.7.2	Similar Software Products	269
7	Computer Crime	281
7.1	Introduction	282
7.2	Hacking	283
7.2.1	What is “Hacking”?	283
7.2.2	Hactivism, or Political Hacking	290
7.2.3	The Law	293
7.2.4	Catching Hackers	294
7.2.5	Penalties Appropriate to the Crime	298
7.2.6	Security	301
7.3	Online Scams	307
7.3.1	Auctions	307
7.3.2	Stock Fraud	309
7.4	Fraud, Embezzlement, Sabotage, Information Theft, and Forgery	310
7.4.1	Credit Cards, Identity Theft, Cell Phones, and More	310
7.4.2	Swindling and Sabotaging Employers and Competitors	315
7.4.3	Swindling the Customer	317
7.4.4	Digital Forgery	317
7.5	Crime Fighting Versus Privacy and Civil Liberties	319
7.5.1	Scanning for Scams	319
7.5.2	Biometrics	320
7.5.3	Search and Seizure of Computers	321
7.5.4	The Cybercrime Treaty	321
8	Computers and Work	329
8.1	The Changing Nature of Work	330
8.2	The Impact on Employment	330
8.2.1	Job Destruction and Creation	330
8.2.2	Changing Skills and Jobs	337
8.3	The Work Environment	340
8.3.1	Teleworking	340
8.3.2	Changing Business Structures	343
8.4	Employee Monitoring	345
8.4.1	Background	345
8.4.2	Data Entry, Phone Work, and Retail	346
8.4.3	Location Monitoring	348
8.4.4	Employee E-mail, Web surfing, and Voice Mail	349
8.5	Health Issues	353
8.5.1	Repetitive Strain Injury	354

9	Broader Issues on the Impact and Control of Computers	365
9.1	Computers and Community	366
9.2	Information Haves and Have-Nots: The Access Issue	371
9.3	Loss of Skills and Judgment	375
9.4	Evaluations of the Impact of Computer Technology	379
9.4.1	The Neo-Luddite View of Computers, Technology, and Human Needs . . .	379
9.4.2	Accomplishments of Technology	385
9.4.3	Who Benefits Most?	386
9.5	Prohibiting Bad Technologies	388
9.5.1	Why and How?	388
9.5.2	The Difficulty of Prediction	390
9.5.3	A Few Observations	392
10	Professional Ethics and Responsibilities	401
10.1	Ethics	403
10.1.1	What Is “Computer Ethics”?	403
10.1.2	What Is Ethics, Anyway?	404
10.1.3	A Variety of Ethical Views	406
10.1.4	Some Important Distinctions	409
10.2	Ethical Guidelines for Computer Professionals	412
10.2.1	Special Aspects of Professional Ethics	412
10.2.2	Professional Codes, Guidelines, and Responsibilities	414
10.3	Cases	418
10.3.1	Introduction and Methodology	418
10.3.2	Copying an Employee’s Files	420
10.3.3	Insufficient Privacy Protection	421
10.3.4	Risky Systems	422
10.3.5	Going Public	424
10.3.6	Release of Personal Information	426
10.3.7	Conflict of Interest	427
10.3.8	A Test Plan	428
10.3.9	Copyright Violation	429
10.3.10	Hiring Foreign Programmers	429
	Epilogue	439
A	The Software Engineering Code and the ACM Code	441
A.1	The Software Engineering Code of Ethics and Professional Practice	441
A.2	The ACM Code of Ethics and Professional Conduct	446

