
Contents

1	History of Computing	1
1.1	Historical Development of Computing and Information Technology	1
1.1.1	Before AD 1900	1
1.1.2	After AD 1900	3
1.1.3	The Development of the Microprocessor	5
1.1.4	Historical Development of Computer Software and the Personal Computer (PC)	5
1.2	Development of the Internet	6
1.3	Development of the World Wide Web	7
1.4	The Emergence of Social and Ethical Problems in Computing	8
1.4.1	The Emergence of Computer Crimes	8
1.4.2	The Present Status: An Uneasy Cyberspace	9
1.5	The Case for Computer Ethics Education	10
1.5.1	What Is Computer Ethics?	10
1.5.2	Why You Should Study Computer Ethics	11
	References	12
2	Morality and the Law	15
2.1	Introduction	16
2.2	Morality	17
2.2.1	Moral Theories	18
2.2.2	Moral Decision Making	18
2.2.3	Moral Codes	19
2.2.4	Moral Standards	21
2.2.5	Guilt and Conscience	22
2.2.6	Morality and Religion	23
2.3	Law	23
2.3.1	The Natural Law	24
2.3.2	Conventional Law	25
2.3.3	The Purpose of Law	25
2.3.4	The Penal Code	26

2.3.5	Morality and the Law	26
2.3.6	Issues for Discussion	28
2.4	Morality, Etiquettes, and Manners	28
2.4.1	Issues for Discussion	28
	References	29
3	Ethics and Ethical Analysis	31
3.1	Traditional Definition	33
3.2	Ethical Theories	33
3.2.1	Consequentialism	34
3.2.2	Deontology	34
3.2.3	Human Nature	35
3.2.4	Relativism	35
3.2.5	Hedonism	35
3.2.6	Emotivism	35
3.3	Functional Definition of Ethics	37
3.4	Ethical Reasoning and Decision Making	38
3.4.1	A Framework for Ethical Decision Making	39
3.4.2	Making and Evaluating Ethical Arguments	39
3.5	Codes of Ethics	41
3.5.1	Preamble	41
3.5.2	Objectives of Codes of Ethics	49
3.6	Reflections on Computer Ethics	50
3.6.1	New Wine in an Old Bottle	50
3.7	Technology and Values	52
3.7.1	Issues for Discussion	53
	References	54
4	Ethics and the Professions	55
4.1	Introduction	56
4.2	Evolution of Professions	56
4.2.1	Origins of Professions	56
4.2.2	Requirements of a Professional	57
4.2.3	Pillars of Professionalism	60
4.3	The Making of an Ethical Professional: Education and Licensing	63
4.3.1	Formal Education	64
4.3.2	Licensing Authorities	65
4.3.3	Professional Codes of Conduct	66
4.4	Professional Decision Making and Ethics	68
4.4.1	Professional Dilemma in Decision Making	69
4.4.2	Guilt and Making Ethical Decisions	70

4.5	Professionalism and Ethical Responsibilities	71
4.5.1	Whistle-Blowing	72
4.5.2	Harassment and Discrimination	74
4.5.3	Ethical and Moral Implications	75
	References.	76
5	Anonymity, Security, Privacy, and Civil Liberties	79
5.1	Introduction	81
5.2	Anonymity	82
5.2.1	Anonymity and the Internet.	82
5.2.2	Advantages and Disadvantages of Anonymity.	83
5.2.3	Legal View of Anonymity.	84
5.3	Security	84
5.3.1	Physical Security	85
5.3.2	Physical Access Controls.	85
5.3.3	Information Security Controls	87
5.3.4	Operational Security	90
5.4	Privacy	90
5.4.1	Definition	90
5.4.2	Types of Privacy	91
5.4.3	Value of Privacy	92
5.4.4	Privacy Implications of Database System	93
5.4.5	Privacy Violations and Legal Implications	94
5.4.6	Privacy Protection and Civil Liberties	97
5.5	Ethical and Legal Framework for Information	99
5.5.1	Ethics and Privacy.	99
5.5.2	Ethical and Legal Basis for Privacy Protection	100
	References.	101
6	Intellectual Property Rights and Computer Technology.	103
6.1	Definitions	104
6.2	Computer Products and Services.	104
6.3	Foundations of Intellectual Property	107
6.3.1	Copyrights.	107
6.3.2	Patents.	110
6.3.3	Trade Secrets.	111
6.3.4	Trademarks	112
6.3.5	Personal Identity	115
6.4	Ownership	116
6.4.1	The Politics of Ownership.	116
6.4.2	The Psychology of Ownership.	117
6.5	Intellectual Property Crimes	118
6.5.1	Infringement	118

6.5.2	The First Sale Doctrine	119
6.5.3	The Fair Use Doctrine	119
6.6	Protection of Ownership Rights	120
6.6.1	Domain of Protection	120
6.6.2	Source and Types of Protection	121
6.6.3	Duration of Protection	122
6.6.4	Strategies of Protection	122
6.7	Protecting Computer Software Under the IP	122
6.7.1	Software Piracy	123
6.7.2	Protection of Software Under Copyright Laws	123
6.7.3	Protection of Software Under Patent Laws	124
6.7.4	Protection of Software Under Trademarks	125
6.7.5	Protection of Software Under Trade Secrets	125
6.8	Transnational Issues and Intellectual Property	126
6.8.1	Issues for Discussion	127
	References	128
7	Social Context of Computing	129
7.1	Introduction	130
7.2	The Digital Divide	131
7.2.1	Access	131
7.2.2	Technology	139
7.2.3	Humanware (Human Capacity)	142
7.2.4	Infrastructure	143
7.2.5	Enabling Environments	143
7.3	Obstacles to Overcoming the Digital Divide	144
7.4	ICT in the Workplace	145
7.4.1	The Electronic Office	145
7.4.2	Office on Wheels and Wings	146
7.4.3	The Virtual Workplace	146
7.4.4	The Quiet Revolution: The Growth of Telecommuting	147
7.4.5	Employee Social and Ethical Issues	151
7.5	Employee Monitoring	152
7.5.1	Workplace Privacy and Surveillance	153
7.5.2	Electronic Monitoring	156
7.6	Workplace, Employee, Health, and Productivity	159
7.6.1	Ergonomics	159
	References	162
8	Software Issues: Risks and Liabilities	165
8.1	Definitions	166
8.1.1	Standards	166
8.1.2	Reliability	167

8.1.3	Security	168
8.1.4	Safety	169
8.1.5	Quality	169
8.1.6	Quality of Service	170
8.2	Causes of Software Failures	170
8.2.1	Human Factors	170
8.2.2	Nature of Software: Complexity	171
8.3	Risk	172
8.3.1	Risk Assessment and Management	173
8.3.2	Risks and Hazards in Workplace Systems	174
8.3.3	Historic Examples of Software Risks	175
8.4	Consumer Protection.	181
8.4.1	Buyer and Provider Rights	182
8.4.2	A Service Provider–User Contract.	184
8.4.3	The Tort Option	185
8.5	Improving Software Quality	187
8.5.1	Techniques for Improving Software Quality	187
8.6	Producer Protection.	188
	References.	189
9	Computer Crimes	191
9.1	Introduction	192
9.2	History of Computer Crimes.	193
9.3	Types of Computer Systems Attacks	195
9.3.1	Penetration.	195
9.3.2	Denial of Service.	197
9.4	Motives of Computer Crimes	197
9.5	Costs and Social Consequences	199
9.5.1	Lack of Cost Estimate Model for Cyberspace Attacks	202
9.5.2	Social and Ethical Consequences.	203
9.6	Computer Crime Prevention Strategies	204
9.6.1	Protecting Your Computer.	204
9.6.2	The Computer Criminal.	205
9.6.3	The Innocent Victim	206
	References.	207
10	New Frontiers for Computer Ethics: Artificial Intelligence	211
10.1	Introduction	212
10.2	Artificial Intelligence	213
10.2.1	Advances in Artificial Intelligence.	214
10.2.2	Artificial Intelligence and Ethics	215
10.2.3	The Future Role of Autonomous Agents.	217
	References.	219

11	New Frontiers for Computer Ethics: Virtualization and Virtual Reality	221
11.1	Virtualization	221
11.2	Different Aspects of Virtualization	222
11.3	Virtualization of Computing Resources	222
11.3.1	History of Computing Virtualization	223
11.3.2	Computing Virtualization Terminologies	224
11.3.3	Types of Computing System Virtualization	225
11.3.4	The Benefits of Computing Virtualization	228
11.4	Virtual Reality	231
11.4.1	Different Types of Virtual Reality	232
11.4.2	Virtualization and Ethics	233
11.5	Social and Ethical Implication of Virtualization	235
11.6	Virtualization Security as an Ethical Imperative	236
11.6.1	Hypervisor Security	237
11.6.2	Securing Communications Between Desktop and Virtual Environment	237
11.6.3	Security of Communication Between Virtual Environments	237
11.6.4	Threats and Vulnerabilities Originating from a Virtual Environment	238
	References	239
12	New Frontiers for Computer Ethics: Cyberspace	241
12.1	Introduction	242
12.2	Cyberspace and the Concepts of Telepresence and Immersion	243
12.3	Securing Cyberspace	244
12.3.1	Detecting Attacks in Cyberspace	244
12.3.2	Cyberspace Systems Survivability	247
12.4	Intellectual Property Rights in Cyberspace	248
12.4.1	Copyrights	251
12.4.2	Patents	252
12.4.3	Trade Secrets	252
12.4.4	Trademarks	253
12.4.5	Personal Identity	254
12.5	Regulating and Censoring Cyberspace	255
12.6	The Social Value of Cyberspace	257
12.7	Privacy in Cyberspace	258
12.7.1	Privacy Protection	259
12.8	Global Cyberethics	259
12.9	Cyberspace Lingua Franca	260
12.10	Global Cyber Culture	261
	References	263

13 Cyberbullying	265
13.1 Definition	265
13.1.1 Legal Definition	266
13.1.2 Cyberstalking	266
13.1.3 Cyber Harassment	267
13.2 Types of Cyberbullying	267
13.2.1 Harassment	267
13.2.2 Flaming	267
13.2.3 Exclusion	268
13.2.4 Outing	268
13.2.5 Masquerading	268
13.3 Areas of Society Most Affected by Cyberbullying	268
13.3.1 Schools	268
13.3.2 Cyberbullying in the Workplace	269
13.4 Legislation Against Cyberbullying	269
13.4.1 Federal Laws	270
13.4.2 State Laws	270
13.4.3 International Laws	271
13.5 Effects of Cyberbullying	271
13.6 Dealing with Cyberbullying	272
13.6.1 Awareness	272
13.6.2 Legislations	272
13.6.3 Community Support	273
13.7 Resources	273
References	275
14 Internet of Things (IoT): Growth, Challenges, and Security	277
14.1 Introduction	277
14.2 Overview and Growth of Internet of Things	279
14.3 Architecture and Networking of IoT	280
14.3.1 Architecture and Protocol Stack of IoTs	281
14.3.2 Challenges of Using TCP/IP Architecture Over the IoT	283
14.4 IoT Governance, Privacy, and Security Challenges	286
14.4.1 Governance and Privacy Concerns	286
14.4.2 Security Challenges	287
14.4.3 Autonomy	288
14.4.4 Computational Constraints	289
14.4.5 Discovery	289
14.4.6 Trust Relationships	289
References	291

15	Ethical, Privacy, and Security Issues in the Online Social Network	
	Ecosystems	293
15.1	Introduction	293
15.2	Introduction to Computer Networks	293
	15.2.1 Computer Network Models	294
	15.2.2 Computer Network Types	296
15.3	Social Networks (SNs)	297
15.4	Online Social Networks (OSNs)	299
	15.4.1 Types of Online Social Networks	299
	15.4.2 Online Social Networking Services	300
	15.4.3 The Growth of Online Social Networks	301
15.5	Ethical and Privacy Issues in Online Social Networks	303
	15.5.1 Privacy Issues in OSNs	303
	15.5.2 Strengthening Privacy in OSNs	306
	15.5.3 Ethical Issues in Online Social Networks	307
15.6	Security and Crimes in Online Social Networks	310
	15.6.1 Beware of Ways to Perpetuate Crimes in Online Social Networks	311
	15.6.2 Defense Against Crimes in Online Social Networks . . .	313
15.7	Proven Security Protocols and Best Practices in Online Social Networks	317
	15.7.1 Authentication	317
	15.7.2 Access Control	317
	15.7.3 Legislation	318
	15.7.4 Self-regulation	318
	15.7.5 Detection	318
	15.7.6 Recovery	318
	References	319
16	Mobile Systems and Their Intractable Social, Ethical and Security Issues	321
16.1	Introduction	321
16.2	Role of Operating Systems in the Growth of the Mobile Ecosystem	322
	16.2.1 Android	323
	16.2.2 iOS	324
	16.2.3 Windows mOS	324
	16.2.4 BlackBerry mOS	324
	16.2.5 Other Smaller mOS	325
16.3	Ethical and Privacy Issues in Mobile Ecosystems	326
16.4	Security Issues in Mobile Ecosystems	327
	16.4.1 Application-Based Threats	328
	16.4.2 Web-Based Threats	329
	16.4.3 Network Threats	330

16.4.4	Physical Threats	330
16.4.5	Operating System-Based Threats	330
16.5	General Mobile Devices Attack Types	331
16.6	Mitigation of Mobile Devices Attacks	334
16.6.1	Mobile Device Encryption	335
16.6.2	Mobile Remote Wiping	336
16.6.3	Mobile Passcode Policy	336
16.7	Users' Role in Securing Mobile Devices	337
	References	337
17	Computer Crime Investigations and Ethics	339
17.1	Introduction	339
17.2	Digital Evidence	340
17.2.1	Looking for Digital Evidence	341
17.2.2	Digital Evidence: Previewing and Acquisition	341
17.3	Preserving Evidence	344
17.4	Analysis of Digital Evidence	344
17.4.1	Analyzing Data Files	345
17.4.2	Analysis Based on Operating Systems	346
17.4.3	Analysis Based on Digital Media	347
17.5	Relevance and Validity of Digital Evidence	350
17.6	Writing Investigative Reports	350
17.7	Ethical Implications and Responsibilities in Computer Forensic Investigations	351
	References	353
18	Biometric Technologies and Ethics	355
18.1	Introduction and Definitions	356
18.1.1	Definitions	357
18.2	The Biometric Authentication Process	358
18.3	Biometric System Components	359
18.3.1	Data Acquisition	359
18.3.2	Enrollments	359
18.3.3	Signal Processing	360
18.3.4	Decision Policy	360
18.4	Types of Biometric Technologies	360
18.4.1	Finger Biometrics	360
18.4.2	Hand Geometry	363
18.4.3	Face Biometrics	363
18.4.4	Voice Biometrics	364
18.4.5	Handwriting Analysis	365
18.4.6	Iris Biometrics	365
18.4.7	Retina	366

18.5 Ethical Implications of Biometric Technologies	366
18.5.1 Issues for Discussion	367
18.6 The Future of Biometrics	367
References	369
Appendix A: The Digital Millennium Copyright Act	371
Appendix B: The Federal False Claims Act	383
Appendix C: Projects	405
Index	409

Ethical and Social Issues in the Information Age

Kizza, J.M.

2017, XXII, 413 p. 22 illus., Hardcover

ISBN: 978-3-319-70711-2