# TABLE OF CONTENTS

**PREFACE**  xvii  
- New to the *Fifth Edition*  xviii  
- Audience and Scope  xix  
- Organization and Structure of the Book  xx  
- The Web Site for *Ethics and Technology*  xxii  
- A Note to Students  xxiii  
- Note to Instructors: A Roadmap for Using This Book  xxiii  
- A Note to Computer Science Instructors  xxiv  
- Acknowledgments  xxv  

**FOREWORD**  xxvii  

**CHAPTER 1**  
**INTRODUCTION TO CYBERETHICS: CONCEPTS, PERSPECTIVES, AND METHODOLOGICAL FRAMEWORKS**  1  
- Scenario 1–1: Hacking into the Mobile Phones of Celebrities  1  
  1.1 Defining Key Terms: Cyberethics and Cybertechnology  2  
  1.1.1 What Is Cybertechnology?  3  
  1.1.2 Why the Term Cyberethics?  3  
  1.2 The Cyberethics Evolution: Four Developmental Phases in Cybertechnology  4  
  1.3 Are Cyberethics Issues Unique Ethical Issues?  7  
  1.3.1 Distinguishing between Unique Technological Features and Unique Ethical Issues  9  
  1.3.2 An Alternative Strategy for Analyzing the Debate about the Uniqueness of Cyberethics Issues  10  
  1.3.3 A Policy Vacuum in Duplicating Computer Software  10  
  1.4 Cyberethics as a Branch of Applied Ethics: Three Distinct Perspectives  12  
  1.4.1 Perspective #1: Cyberethics as a Field of Professional Ethics  12  
  1.4.2 Perspective #2: Cyberethics as a Field of Philosophical Ethics  14  
  1.4.3 Perspective #3: Cyberethics as a Field of Sociological/Descriptive Ethics  16  
- Scenario 1–2: Developing the Code for a Computerized Weapon System  8  
- Scenario 1–3: Digital Piracy  8  
  1.3.1 Distinguishing between Unique Technological Features and Unique Ethical Issues  9  
  1.3.2 An Alternative Strategy for Analyzing the Debate about the Uniqueness of Cyberethics Issues  10  
  1.3.3 A Policy Vacuum in Duplicating Computer Software  10  
- Scenario 1–4: The Impact of Technology X on the Pleasantville Community  17  
  1.5 A Comprehensive Cyberethics Methodology  19  
  1.5.1 A “Disclosive” Method for Cyberethics  19  
  1.5.2 An Interdisciplinary and Multilevel Method for Analyzing Cyberethics Issues  21  
- 1.6 A Comprehensive Strategy for Approaching Cyberethics Issues  21  
  1.7 Chapter Summary  22  
- Review Questions  23  
- Discussion Questions  23  
- Scenarios for Analysis  23  
- Endnotes  24  
- References  25  
- Further Readings  26  
- Online Resources  26
CHAPTER 2
ETHICAL CONCEPTS AND ETHICAL THEORIES: FRAMEWORKS FOR ANALYZING MORAL ISSUES

Scenario 2–1: The Case of the “Runaway Trolley”: A Classic Moral Dilemma

2.1 Ethics and Morality
   2.1.1 What Is Morality? 29
   2.1.2 The Study of Morality: Three Distinct Approaches for Evaluating and Justifying the Rules Comprising a Moral System 32

2.2 Discussion Stoppers as Roadblocks to Moral Discourse
   2.2.1 Discussion Stopper #1: People Disagree on Solutions to Moral Issues 36
   2.2.2 Discussion Stopper #2: Who Am I to Judge Others? 37
   2.2.3 Discussion Stopper #3: Morality Is Simply a Private Matter 39
   2.2.4 Discussion Stopper #4: Morality Is Simply a Matter for Individual Cultures to Decide 40

Scenario 2–2: The Price of Defending Moral Relativism 41

2.3 Why Do We Need Ethical Theories? 43

2.4 Consequence-Based Ethical Theories
   2.4.1 Act Utilitarianism 46

Scenario 2–3: A Controversial Policy in Newmerica 46
   2.4.2 Rule Utilitarianism 46

2.5 Duty-Based Ethical Theories
   2.5.1 Rule Deontology 48

Scenario 2–4: Making an Exception for Oneself 48
   2.5.2 Act Deontology 49

Scenario 2–5: A Dilemma Involving Conflicting Duties 50

2.6 Contract-Based Ethical Theories
   2.6.1 Some Criticisms of Contract-Based Theories 52
   2.6.2 Rights-Based Contract Theories 53

2.7 Character-Based Ethical Theories
   2.7.1 Being a Moral Person vs. Following Moral Rules 54
   2.7.2 Acquiring the “Correct” Habits 55

2.8 Integrating Aspects of Classical Ethical Theories into a Single Comprehensive Theory
   2.8.1 Moor's Just-Consequentialist Theory and Its Application to Cybertechnology 57
   2.8.2 Key Elements in Moor's Just-Consequentialist Framework 58

2.9 Chapter Summary 59

Review Questions 59
Discussion Questions 60
Scenarios for Analysis 60
Endnotes 61
References 61
Further Readings 62

CHAPTER 3
CRITICAL REASONING SKILLS FOR EVALUATING DISPUTES IN CYBERETHICS

SCENARIO 3–1: Reasoning About Whether to Download Software from “Sharester” 63

3.1 What Is Critical Reasoning? 64
   3.1.1 Some Basic Concepts: (Logical) Arguments and Claims 64
   3.1.2 The Role of Arguments 65
   3.1.3 The Basic Structure of an Argument 65

3.2 Constructing an Argument 67

3.3 Valid Arguments 68

3.4 Sound Arguments 71

3.5 Invalid Arguments 73

3.6 Inductive Arguments 74

3.7 Fallacious Arguments 75
5.2 What Is Personal Privacy? 117
  5.2.1 Accessibility Privacy: Freedom from Unwarranted Intrusion 118
  5.2.2 Decisional Privacy: Freedom from Interference in One’s Personal Affairs 118
  5.2.3 Informational Privacy: Control over the Flow of Personal Information 118
  5.2.4 A Comprehensive Account of Privacy 119
Scenario 5–2: Descriptive Privacy 119
Scenario 5–3: Normative Privacy 120
  5.2.5 Privacy as “Contextual Integrity” 120
Scenario 5–4: Preserving Contextual Integrity in a University Seminar 121
5.3 Why Is Privacy Important? 121
  5.3.1 Is Privacy an Intrinsic Value? 122
  5.3.2 Privacy as a Social Value 123
5.4 Gathering Personal Data: Surveillance, Recording, and Tracking Techniques 123
  5.4.1 “Dataveillance” Techniques 124
  5.4.2 Internet Cookies 124
  5.4.3 RFID Technology 125
  5.4.4 Cybertechnology and Government Surveillance 126
5.5 Analyzing Personal Data: Big Data, Data Mining, and Web Mining 127
  5.5.1 Big Data: What, Exactly, Is It, and Why Does It Threaten Privacy? 128
  5.5.2 Data Mining and Personal Privacy 128
Scenario 5–5: Data Mining at the XYZ Credit Union 129
  5.5.3 Web Mining: Analyzing Personal Data Acquired from Our Interactions Online 132
5.6 Protecting Personal Privacy in Public Space 132
  5.6.1 PPI vs. NPI 133
Scenario 5–6: Shopping at SuperMart 133
Scenario 5–7: Shopping at Nile.com 134
  5.6.2 Search Engines and the Disclosure of Personal Information 135
5.7 Privacy Legislation and Industry Self-Regulation 137
  5.7.1 Industry Self-Regulation and Privacy-Enhancing Tools 137
  5.7.2 Privacy Laws and Data Protection Principles 139
5.8 A Right to “Be Forgotten” (or to “Erasure”) in the Digital Age 140
Scenario 5–8: An Arrest for an Underage Drinking Incident 20 Years Ago 141
  5.8.1 Arguments Opposing RTBF 142
  5.8.2 Arguments Defending RTBF 143
  5.8.3 Establishing “Appropriate” Criteria 144
5.9 Chapter Summary 146
Review Questions 146
Discussion Questions 147
Scenarios for Analysis 148
Endnotes 148
References 149
Further Readings 150

CHAPTER 6
SECURITY IN CYBERSPACE 151

Scenario 6–1: The “Olympic Games” Operation and the Stuxnet Worm 151
6.1 Security in the Context of Cybertechnology 152
  6.1.1 Cybersecurity as Related to Cybercrime 153
  6.1.2 Security and Privacy: Some Similarities and Some Differences 153
6.2 Three Categories of Cybersecurity 154
  6.2.1 Data Security: Confidentiality, Integrity, and Availability of Information 155
  6.2.2 System Security: Viruses, Worms, and Malware 156
  6.2.3 Network Security: Protecting our Infrastructure 156
Scenario 6–2: The “GhostNet” Controversy 157
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3</td>
<td>6.3.1</td>
<td>Deployment and Service/Delivery Models for the Cloud</td>
<td>158</td>
</tr>
<tr>
<td></td>
<td>6.3.2</td>
<td>Securing User Data Residing in the Cloud</td>
<td>159</td>
</tr>
<tr>
<td></td>
<td>6.3.3</td>
<td>Assessing Risk in the Cloud and in the Context of Cybersecurity</td>
<td>160</td>
</tr>
<tr>
<td>6.4</td>
<td>6.4.1</td>
<td>What Is “The Hacker Ethic”?</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>6.4.2</td>
<td>Are Computer Break-ins Ever Ethically Justifiable?</td>
<td>163</td>
</tr>
<tr>
<td>6.5</td>
<td>6.5.1</td>
<td>Cyberterrorism vs. Hacktivism</td>
<td>165</td>
</tr>
<tr>
<td>6.6</td>
<td>6.6.1</td>
<td>Information Warfare vs. Conventional Warfare</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td>6.6.2</td>
<td>Potential Consequences for Nations that Engage in IW</td>
<td>168</td>
</tr>
<tr>
<td>6.7</td>
<td></td>
<td>Chapter Summary</td>
<td>170</td>
</tr>
</tbody>
</table>

Review Questions 170
Discussion Questions 171
Scenarios for Analysis 171
Endnotes 171
References 172
Further Readings 174

CHAPTER 7

CYBERCRIME AND CYBER-RELATED CRIMES 175

Scenario 7–1: Creating a Fake Facebook Account to Catch Criminals 175
7.1 Cybercrimes and Cybercriminals 177
7.1.1 Background Events: A Brief Sketch 177
7.1.2 A Typical Cybercriminal 178
7.2 Hacking, Cracking, and Counter Hacking 178
7.2.1 Hacking vs. Cracking 179
7.2.2 Active Defense Hacking: Can Acts of “Hacking Back” or Counter Hacking Ever Be Morally Justified? 179
7.3 Defining Cybercrime 180
7.3.1 Determining the Criteria 181
7.3.2 A Preliminary Definition of Cybercrime 181
7.3.3 Framing a Coherent and Comprehensive Definition of Cybercrime 182
7.4 Three Categories of Cybercrime: Piracy, Trespass, and Vandalism in Cyberspace 183
7.5 Cyber-Related Crimes 184
7.5.1 Some Examples of Cyber-Exacerbated vs. Cyber-Assisted Crimes 184
7.5.2 Identity Theft 185
7.6 Technologies and Tools for Combating Cybercrime 187
7.6.1 Biometric Technologies 187
7.6.2 Keystroke-Monitoring Software and Packet-Sniffing Programs 188
7.7 Programs and Techniques Designed to Combat Cybercrime in the United States 189
7.7.1 Entrapment and “Sting” Operations to Catch Internet Pedophiles 189
Scenario 7–2: Entrapment on the Internet 189
7.7.2 Enhanced Government Surveillance Techniques and the Patriot Act 189
7.8 National and International Laws to Combat Cybercrime 190
7.8.1 The Problem of Jurisdiction in Cyberspace 190
Scenario 7–3: A Virtual Casino 191
Scenario 7–4: Prosecuting a Computer Corporation in Multiple Countries 192
7.8.2 Some International Laws and Conventions Affecting Cybercrime 192
Scenario 7–5: The Pirate Bay Web Site 193
7.9 Cybercrime and the Free Press: The Wikileaks Controversy 193
CHAPTER 8
INTELLECTUAL PROPERTY DISPUTES IN CYBERSPACE 201

Scenario 8–1: Streaming Music Online 201
8.1.1 Intellectual Objects 203
8.1.2 Why Protect Intellectual Objects? 203
8.1.3 Software as Intellectual Property 204
8.1.4 Evaluating a Popular Argument Used by the Software Industry to Show Why It Is Morally Wrong to Copy Proprietary Software 205
8.2 Copyright Law and Digital Media 206
8.2.1 The Evolution of Copyright Law in the United States 206
8.2.2 The Fair-Use and First-Sale Provisions of Copyright Law 207
8.2.3 Software Piracy as Copyright Infringement 208
8.2.4 Napster and the Ongoing Battles over Sharing Digital Music 209
8.3 Patents, Trademarks, and Trade Secrets 212
8.3.1 Patent Protections 212
8.3.2 Trademarks 213
8.3.3 Trade Secrets 214
8.4 Jurisdictional Issues Involving Intellectual Property Laws 214
8.5 Philosophical Foundations for Intellectual Property Rights 215
8.5.1 The Labor Theory of Property 215
Scenario 8–2: DEF Corporation vs. XYZ Inc. 216
8.5.2 The Utilitarian Theory of Property 216
Scenario 8–3: Sam’s e-Book Reader Add-on Device 217
8.5.3 The Personality Theory of Property 217
Scenario 8–4: Angela’s B++ Programming Tool 218
8.6 The “Free Software” and “Open Source” Movements 219
8.6.1 GNU and the Free Software Foundation 219
8.6.2 The “Open Source Software” Movement: OSS vs. FSF 220
8.7 The “Common Good” Approach: An Alternative Framework for Analyzing the Intellectual Property Debate 221
8.7.1 Information Wants to be Shared vs. Information Wants to be Free 223
8.7.2 Preserving the Information Commons 225
8.7.3 The Fate of the Information Commons: Could the Public Domain of Ideas Eventually Disappear? 226
8.7.4 The Creative Commons 227
8.8 PIPA, SOPA, and RWA Legislation: Current Battlegrounds in the Intellectual Property War 228
8.8.1 The PIPA and SOPA Battles 228
8.8.2 RWA and Public Access to Health-Related Information 229
Scenario 8–5: Elsevier Press and “The Cost of Knowledge” Boycott 229
8.8.3 Intellectual Property Battles in the Near Future 231
8.9 Chapter Summary 231
Review Questions 231
### Table of Contents

10.3 Cybertechnology and Race 271  
   10.3.1 Internet Usage Patterns 272  
   10.3.2 Racism and the Internet 272  
10.4 Cybertechnology and Gender 273  
   10.4.1 Access to High-Technology Jobs 274  
   10.4.2 Gender Bias in Software Design and Video Games 275  
10.5 Cybertechnology, Democracy, and Democratic Ideals 276  
   10.5.1 Has Cybertechnology Enhanced or Threatened Democracy? 276  
   10.5.2 How has Cybertechnology Affected Political Elections in Democratic Nations? 279  
10.6 The Transformation and the Quality of Work 280  
   10.6.1 Job Displacement and the Transformed Workplace 281  
   10.6.2 The Quality of Work Life in the Digital Era 283  

Scenario 10–3: Employee Monitoring and the Case of Ontario vs. Quon 284  

10.7 Chapter Summary 287  
Review Questions 287  
Discussion Questions 288  
Scenarios for Analysis 288  
Endnotes 289  
References 289  
Further Readings 291

## CHAPTER 11

**ONLINE COMMUNITIES, VIRTUAL REALITY, AND ARTIFICIAL INTELLIGENCE** 292  

Scenario 11–1: Ralph’s Online Friends and Artificial Companions 292  
11.1 Online Communities and Social Networking Services 293  
   11.1.1 Online Communities vs. Traditional Communities 294  
   11.1.2 Blogs and Some Controversial Aspects of the Bogosphere 295  

Scenario 11–2: “The Washingtonienne” Blogger 295  
   11.1.3 Some Pros and Cons of SNSs (and Other Online Communities) 296  

Scenario 11–3: A Suicide Resulting from Deception on MySpace 298  
11.2 Virtual Environments and Virtual Reality 299  
   11.2.1 What Is Virtual Reality (VR)? 300  
   11.2.2 Ethical Aspects of VR Applications 301  
11.3 Artificial Intelligence (AI) 305  
   11.3.1 What Is AI? A Brief Overview 305  
   11.3.2 The Turing Test and John Searle’s “Chinese Room” Argument 306  
   11.3.3 Cyborgs and Human–Machine Relationships 307  
11.4 Extending Moral Consideration to AI Entities 310  
   11.4.1 Determining Which Kinds of Beings/Entities Deserve Moral Consideration 310  
   11.4.2 Moral Patients vs. Moral Agents 311  

Scenario 11–4: Artificial Children 310  
11.5 Chapter Summary 312  
Review Questions 313  
Discussion Questions 313  
Scenarios for Analysis 313  
Endnotes 314  
References 315  
Further Readings 316

## CHAPTER 12

**ETHICAL ASPECTS OF EMERGING AND CONVERGING TECHNOLOGIES** 317  

Scenario 12–1: When “Things” Communicate with One Another 317  
12.1 Converging Technologies and Technological Convergence 318  
12.2 Ambient Intelligence (AmI) and Ubiquitous Computing 319
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2.1</td>
<td>Pervasive Computing, Ubiquitous Communication, and Intelligent User Interfaces</td>
<td>320</td>
</tr>
<tr>
<td>12.2.2</td>
<td>Ethical and Social Aspects of AmI</td>
<td>321</td>
</tr>
<tr>
<td>Scenario 12–2:</td>
<td>E. M. Forster’s “(Pre)Cautionary Tale”</td>
<td>322</td>
</tr>
<tr>
<td>Scenario 12–3: Jeremy Bentham’s “Panopticon/Inspection House” (Thought Experiment)</td>
<td>323</td>
<td></td>
</tr>
<tr>
<td>12.3</td>
<td>Nanotechnology and Nanocomputing</td>
<td>324</td>
</tr>
<tr>
<td>12.3.1</td>
<td>Nanotechnology: A Brief Overview</td>
<td>324</td>
</tr>
<tr>
<td>12.3.2</td>
<td>Ethical Issues in Nanotechnology and Nanocomputing</td>
<td>326</td>
</tr>
<tr>
<td>12.4</td>
<td>Autonomous Machines</td>
<td>329</td>
</tr>
<tr>
<td>12.4.1</td>
<td>What Is an AM?</td>
<td>329</td>
</tr>
<tr>
<td>12.4.2</td>
<td>Some Ethical and Philosophical Questions Pertaining to AMs</td>
<td>332</td>
</tr>
<tr>
<td>12.5</td>
<td>Machine Ethics and Moral Machines</td>
<td>336</td>
</tr>
<tr>
<td>12.5.1</td>
<td>What Is Machine Ethics?</td>
<td>336</td>
</tr>
<tr>
<td>12.5.2</td>
<td>Designing Moral Machines</td>
<td>337</td>
</tr>
<tr>
<td>12.6</td>
<td>A “Dynamic” Ethical Framework for Guiding Research in New and Emerging Technologies</td>
<td>340</td>
</tr>
<tr>
<td>12.6.1</td>
<td>Is an ELSI‐Like Model Adequate for New/Emerging Technologies?</td>
<td>340</td>
</tr>
<tr>
<td>12.6.2</td>
<td>A “Dynamic Ethics” Model</td>
<td>341</td>
</tr>
<tr>
<td>12.7</td>
<td>Chapter Summary</td>
<td>341</td>
</tr>
<tr>
<td>Review Questions</td>
<td>342</td>
<td></td>
</tr>
<tr>
<td>Discussion Questions</td>
<td>342</td>
<td></td>
</tr>
<tr>
<td>Scenarios for Analysis</td>
<td>343</td>
<td></td>
</tr>
<tr>
<td>Endnotes</td>
<td>343</td>
<td></td>
</tr>
<tr>
<td>References</td>
<td>344</td>
<td></td>
</tr>
<tr>
<td>Further Readings</td>
<td>346</td>
<td></td>
</tr>
</tbody>
</table>

GLOSSARY 347

INDEX 353