

# TEXTS IN COMPUTER SCIENCE

---

*Editors*

David Gries

Fred B. Schneider

## TEXTS IN COMPUTER SCIENCE

---

*Alagar and Periyasamy*, Specification of Software Systems

*Apt and Olderog*, Verification of Sequential and Concurrent Programs,  
Second Edition

*Back and von Wright*, Refinement Calculus

*Beidler*, Data Structures and Algorithms

*Bergin*, Data Structure Programming

*Brooks*, C Programming: The Essentials for Engineers and Scientists

*Brooks*, Problem Solving with Fortran 90

*Dandamudi*, Fundamentals of Computer Organization and Design

*Dandamudi*, Introduction to Assembly Language Programming

*Fitting*, First-Order Logic and Automated Theorem Proving, Second Edition

*Grillmeyer*, Exploring Computer Science with Scheme

*Homer and Selman*, Computability and Complexity Theory

*Immerman*, Descriptive Complexity

*Jalote*, An Integrated Approach to Software Engineering, Second Edition

*Kozen*, Automata and Computability

*(continued after index)*

Joseph Migga Kizza

# **Ethical and Social Issues in the Information Age**

Third Edition

 Springer

Joseph Migga Kizza  
Computer Science and Electrical Engineering  
University of Tennessee-Chattanooga  
Chattanooga, TN 37403, USA  
joseph-kizza@utc.edu

*Series Editors:*

David Gries  
Department of Computer Science  
415 Boyd Graduate Studies Research Center  
The University of Georgia  
Athens, GA 30602-7404, USA

Fred B. Schneider  
Department of Computer Science  
Upton Hall  
Cornell University  
Ithaca, NY 14853-7501, USA

ISBN-13: 978-1-84628-658-2 e-ISBN-13: 978-1-84628-659-9

Library of Congress Control Number: 2007922975

British Library Cataloguing in Publication Data  
A catalogue record for this book is available from the British Library

© Springer-Verlag London Limited 2007

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

*Cover illustration:* “Mossy Shore” by Pam Clocksin, 2002

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

Springer Science+Business Media

springer.com

*In memory of our mothers:*

*Melesiane Nakatudde and Kevina Nakwoga.*





## PREFACE TO THE THIRD EDITION

As I wrote in my second edition preface, since the publication of the second edition in 2003, there have been tremendous changes in the fields of computer science and information sciences. During this period, we have become more dependent on computer and telecommunication technology than ever before. As we, individually and as nations, become more dependent on cyberspace technology, it has itself, in turn, become a critical component of individual nations' security infrastructures that control power grids, gas and oil storage facilities, transportation and all forms of national communication, including emergency services. This intertwining of security components with cyberspace has elevated it to an important security component for not only individuals but nations as well.

The recent rise in cyberattacks, many of them with lightening speed, affecting millions of computers worldwide and in the process causing billions of dollars in losses to individuals and businesses, is an indication of how unprepared we are to handle such attacks not only now but also in the future. It is also a mark of the poor state of our cyberspace security policies, the cyberspace on which we have come to depend so much, and the vulnerability of us all. The fact that there are no signs yet to indicate that there is going to be a slow down in such attacks, and that nations are doing anything worth calling preventive has heightened the need for an effective strategy to produce responsible professionals who can play an active role in the fight against computer and cyber attacks and vandalism.

As we look for such a strategy, technological development races on with new technologies that make our efforts and existing technologies on which they are based obsolete in shorter and shorter periods. For example, when I started to write the first edition in 1996, computer networking and associated computer network security were not big, the Internet and associated dot-coms were yet to become commercialized and associated with big money, and mass global computer network attacks like “Malissa”, “Love Boy”, and Distributed Denial of Services (DDOS) were unknown.

All these illustrate the speed at which the computing environment is changing and demonstrate a need for continuous review of the computer science education in both content and pedagogy. So the focus in this edition is to address those changes. In this edition, I have made major changes in some of the chapters, reorganized others, and added new ones to bring the book update with current issues.

## RATIONALE FOR THE CHANGES

The following three chapters have been added to this edition:

- (1) Computer Networks and Online Crimes—To cover the basic core knowledge of computer networks for those who are not yet exposed to computer networks. It then discusses the major online crimes and further discusses defense against online crimes. This chapter has been added because since the second edition major computer crimes are now online and the remedies for them are based on the computer network. For a student to understand computer crimes today, a knowledge of computer networks and the jargons that comes with it is necessary.
- (2) Computer Crime Investigation—While we teach the ethics of computer use and discuss the crimes, we must follow that with ways and technologies that are currently being used by law enforcement agencies and others by collecting digital evidence, analyzing it, presenting it in court, and probably apprehending the criminal. This knowledge is what we want the student to acquire in this chapter.



- (3) **Biometrics**—Teaching students about the ethical use of computers and discussing with them the types of major computer crimes and how to mitigate such crimes through use of advanced technologies, also requires a thorough discussion of current and more advanced techniques and technologies in access control. We do this by discussing the most reliable and upcoming technique and associated technologies under biometrics.

## CHAPTER OVERVIEW

The book is now divided into fourteen chapters as follows:

**Chapter 1—Introduction to the Study of Social and Ethical Computing** gives an overview of the history of computing science in hardware, software, and networking. It also discusses the development of computer crimes and the current social and ethical environment. Further, computer ethics is defined, and a need to study computer ethics is emphasized.

**Chapter 2—Morality and the Law** defines and examines personal and public morality, the law, looking at both conventional and natural law, and the intertwining of morality and the law. It, together with chapter 3, gives the reader the philosophical framework needed for the remainder of the book.

**Chapter 3—Ethics, Technology, and Values** builds upon chapter 2 in setting up the philosophical framework for the book discussing moral theories and problems in ethical relativism. Based on these and in light of the rapid advances in technology, the chapter discusses the moral and ethical premises and their corresponding values in the changing technology arena.

**Chapter 4—Ethics and the Professions** examines the changing nature of the professions and how they cope with the impact of technology on their fields. Professional and ethical responsibilities based on community values and the law are also discussed. And social issues including harassment and discrimination are thoroughly covered.

**Chapter 5—Anonymity, Security, and Privacy and Civil Liberties** surveys the traditional ethical issues of privacy, security, anonymity and analyzes how these issues are affected by computer technology. Information gathering, databasing, and civil liberties are also discussed.

**Chapter 6—Intellectual Property Rights and Computer Technology** discusses the foundations of intellectual property rights and how computer technology has influenced and changed the traditional issues of property rights, in particular intellectual property rights.

**Chapter 7—Social Context of Computing** considers the three main social issues in computing namely, the digital divide, workplace issues like employee monitoring, and health risks, and how these issues are changing with the changing computer technology.

**Chapter 8—Software Issues: Risks and Liabilities** revisits property rights, responsibility and accountability with a focus on computer software. The risks and liabilities associated with software and risk assessment are also discussed.

**Chapters 9—Computer Crimes** surveys the history and examples of computer crimes, their types, costs on society, and strategies of detection and prevention.

**Chapter 10—New Frontiers for Ethical Consideration: Artificial Intelligence, Cyberspace, and Virtual Reality** discusses the new frontiers of ethics: virtual reality, artificial intelligence, and the Internet, and how these new frontiers are affecting the traditional ethical and social issues.

**Chapter 11—Cyberspace and Cyberethics** discusses the new realities of global computer networks, the intertwining of global economies, monopolies and their economic implications, globalization, emerging issues like global ethics, culture, and the development of the lingua franca for the Internet.

**Chapter 12—Computer Networks and Online Crimes** begins by presenting the core basics of computer networks for those readers who have never taken a course in computer networks. Then the chapter discusses the major online crimes and ends by a discussion of techniques and technologies in use to mitigate these crimes.

**Chapter 13—Computer Crime Investigations** discusses what constitutes digital evidence, the collection and analysis of digital evidence, chain of custody, the writing of the report, and the possible appearance in court as an expert witness.

**Chapter 14—Biometrics** starts by discussing the different techniques in access control. Biometric technologies and techniques are then introduced to be contrasted with the other known techniques. Several biometrics and biometric technologies are discussed.

## AUDIENCE

This book satisfies the requirements of the new CC2001 Computer Science Curricula for undergraduates: CS265s Social and Professional Issues. Students in related disciplines like computer information and information management systems, and library sciences will also find this book informative.

It is also good for anyone who is concerned with how all traditional ethical and social issues like privacy, civil liberties, security, anonymity, and workplace issues like harassment and discrimination are handled in the new computer technology environment.

In addition, anybody interested in reading about network, computer, and data security, will also find the book very helpful.

## ACKNOWLEDGMENTS

I appreciate all the help I received from colleagues who offered ideas, criticism, and suggested materials. Special thanks to my dear wife, Dr. Immaculate Kizza, who offered a considerable amount of help, constructive ideas, and wonderful support.

*Joseph Migga Kizza*  
*Department of Computer Science and Electrical Engineering*  
*University of Tennessee at Chattanooga*  
*Chattanooga, Tennessee, 2006*



# CONTENTS

PREFACE TO THE THIRD EDITION . . . . .	vii
--	-----

...

## 1

### INTRODUCTION TO SOCIAL AND ETHICAL COMPUTING

<b>1.1</b>	Historical Development of Computing and Information Technology . . . . .	1
1.1.1	Before 1900 AD . . . . .	1
1.1.2	After 1900 AD . . . . .	3
1.1.3	The Development of the Microprocessor . . . . .	6
1.1.4	Historical Development of Computer Software and the Personal Computer (PC) . . . . .	7
<b>1.2</b>	Development of the Internet . . . . .	8
<b>1.3</b>	Development of the World Wide Web. . . . .	10
<b>1.4</b>	The Emergence of Social and Ethical Problems in Computing. . . . .	11
1.4.1	The Emergence of Computer Crimes. . . . .	11
1.4.2	The Present Status: An Uneasy Cyberspace . . . . .	13
<b>1.5</b>	The Case for Computer Ethics Education . . . . .	14
1.5.1	What is Computer Ethics?. . . . .	14
1.5.2	Why You Should Study Computer Ethics . . . . .	15

1.6	References . . . . .	17
1.7	Exercises . . . . .	17

## ... 2 MORALITY AND THE LAW

2.1	Introduction . . . . .	20
2.2	Morality . . . . .	21
2.2.1	Moral Theories . . . . .	21
2.2.2	Moral Decision Making . . . . .	22
2.2.3	Moral Codes . . . . .	23
2.2.4	Moral Standards . . . . .	26
2.2.5	Guilt and Conscience . . . . .	26
2.3	Law . . . . .	28
2.3.1	The Natural Law . . . . .	29
2.3.2	Conventional Law . . . . .	30
2.3.3	The Purpose of Law . . . . .	30
2.3.4	The Penal Code . . . . .	31
2.4	Morality and the Law . . . . .	31
2.5	References . . . . .	34
2.6	Further Reading . . . . .	35
2.7	Exercises . . . . .	35

## ... 3 ETHICS, TECHNOLOGY, AND VALUE

3.1	Traditional Definition of Ethics . . . . .	38
3.2	Ethical Theories . . . . .	39
3.2.1	Consequentialism . . . . .	39
3.2.2	Deontology . . . . .	40
3.2.3	Human Nature . . . . .	41
3.2.4	Relativism . . . . .	41
3.2.5	Hedonism . . . . .	41
3.2.6	Emotivism . . . . .	42
3.3	Functional Definition of Ethics . . . . .	43
3.4	Codes of Ethics . . . . .	45
3.4.1	Objectives of Codes of Ethics . . . . .	57
3.5	Reflections on Computer Ethics . . . . .	57
3.5.1	New Wine in an Old Bottle . . . . .	57

3.6	Technology and Values . . . . .	60
3.7	References . . . . .	62
3.8	Further Reading . . . . .	62
3.9	Exercises . . . . .	63

## ... 4 ETHICS AND THE PROFESSIONS

4.1	Introduction . . . . .	66
4.2	Evolution of Professions . . . . .	66
4.2.1	Origins of Professions . . . . .	66
4.2.2	Requirements of a Professional . . . . .	67
4.2.3	Pillars of Professionalism . . . . .	69
4.3	The Making of an Ethical Professional: Education and Licensing . . . . .	74
4.3.1	Formal Education . . . . .	75
4.3.2	Licensing Authorities . . . . .	76
4.3.3	Professional Codes of Conduct . . . . .	77
4.4	Professional Decision Making and Ethics . . . . .	81
4.4.1	Professional Dilemmas in Decision Making . . . . .	82
4.4.2	Making and Evaluating Ethical Arguments . . . . .	84
4.4.3	Guilt and Making Ethical Decisions . . . . .	86
4.5	Professionalism and Ethical Responsibilities . . . . .	88
4.5.1	Whistle-Blowing . . . . .	88
4.5.2	Harassment and Discrimination . . . . .	92
4.5.3	Ethical and Moral Implications . . . . .	93
4.6	References . . . . .	94
4.7	Further reading . . . . .	95
4.8	Exercises . . . . .	95

## ... 5 ANONYMITY, SECURITY, PRIVACY, AND CIVIL LIBERTIES

5.1	Introduction . . . . .	100
5.2	Anonymity . . . . .	100
5.2.1	Anonymity and the Internet . . . . .	101

5.3 Security ..... 101

5.3.1 Physical Security ..... 102

5.3.2 Information Security ..... 104

5.4 Privacy ..... 108

5.4.1 Definition ..... 108

5.4.2 Value of Privacy ..... 109

5.4.3 Information Gathering, Databases, and Privacy. .... 110

5.4.4 Privacy Violations and Legal Implications ..... 112

5.4.5 Privacy Protection and Civil Liberties ..... 116

5.5 Ethical and Social Issues..... 119

5.5.1 Ethics and Privacy ..... 119

5.5.2 Ethics and Security ..... 120

5.6 References ..... 121

5.7 Further Reading ..... 122

5.8 Exercises..... 122

... 6 INTELLECTUAL PROPERTY RIGHTS  
AND COMPUTER TECHNOLOGY

6.1 Computer Products and Services ..... 126

6.2 Foundations of Intellectual Property Rights..... 129

6.2.1 Copyrights..... 130

6.2.2 Patents ..... 133

6.2.3 Trade Secrets ..... 135

6.2.4 Trademarks ..... 137

6.2.5 Personal Identity..... 140

6.3 Ownership ..... 142

6.3.1 The Politics of Ownership..... 142

6.3.2 The Psychology of Ownership ..... 143

6.4 Infringement..... 144

6.4.1 Copyright Infringement ..... 144

6.4.2 Patent Infringement..... 145

6.4.3 Trademark Infringement ..... 145

6.4.4 The First Sale Doctrine ..... 146

6.4.5 The Fair Use Doctrine ..... 146



<b>6.5</b>	<b>Protection of Ownership Rights</b> . . . . .	147
6.5.1	Domain of Protection. . . . .	147
6.5.2	Source and Types of Protection. . . . .	148
6.5.3	Duration of Protection . . . . .	148
6.5.4	Strategies of Protection. . . . .	148
<b>6.6</b>	<b>The Legal Protection of Computer Software</b> . . . . .	149
6.6.1	Protection Under Copyright Laws. . . . .	150
6.6.2	Protection Under Patent Laws . . . . .	151
6.6.3	Protection Under Trademarks . . . . .	152
6.6.4	Protection Under Trade Secrets . . . . .	152
<b>6.7</b>	<b>References</b> . . . . .	153
<b>6.8</b>	<b>Further Reading</b> . . . . .	154
<b>6.9</b>	<b>Exercises</b> . . . . .	154

## ... 7

## SOCIAL CONTEXT OF COMPUTING

<b>7.1</b>	<b>Introduction</b> . . . . .	158
<b>7.2</b>	<b>The Digital Divide</b> . . . . .	159
7.2.1	Access. . . . .	159
7.2.2	Technology . . . . .	167
7.2.3	Humanware (Human Capacity) . . . . .	170
7.2.4	Infrastructure . . . . .	171
7.2.5	Enabling Environments. . . . .	171
<b>7.3</b>	<b>ICT in the Workplace</b> . . . . .	173
7.3.1	The Electronic Office. . . . .	173
7.3.2	Office on Wheels and Wings . . . . .	174
7.3.3	The Virtual Workplace . . . . .	175
7.3.4	The Home worker: A Growing Concept of Telecommuters. . . . .	176
7.3.5	Employee Social and Ethical Issues . . . . .	182
<b>7.4</b>	<b>Employee Monitoring</b> . . . . .	183
7.4.1	Workplace Privacy and Surveillance . . . . .	185
7.4.2	Electronic Monitoring . . . . .	188
<b>7.5</b>	<b>Workplace Employee Health and Productivity</b> . . . . .	192
7.5.1	Ergonomics . . . . .	193
<b>7.6</b>	<b>References</b> . . . . .	196

7.7 Further Reading . . . . . 198

7.8 Exercises . . . . . 198

... **8** SOFTWARE ISSUES: RISKS AND LIABILITIES

8.1 Definitions . . . . . 202

8.1.1 Standards . . . . . 202

8.1.2 Reliability . . . . . 204

8.1.3 Security . . . . . 205

8.1.4 Safety . . . . . 206

8.1.5 Quality . . . . . 207

8.1.6 Quality of Service (QoS) . . . . . 207

8.2 Causes of Software Failures . . . . . 208

8.2.1 Human Factors . . . . . 208

8.2.2 Nature of Software: Complexity . . . . . 209

8.3 Risk . . . . . 210

8.3.1 Risk Assessment and Management . . . . . 211

8.3.2 Risks and Hazards in Workplace Systems . . . . . 213

8.3.3 Historic Examples of Software Risks . . . . . 214

8.4 Consumer Protection . . . . . 223

8.4.1 Buyers' Rights . . . . . 223

8.4.2 Classification of Computer Software . . . . . 225

8.4.3 The Contract Option . . . . . 229

8.4.4 The Tort Option . . . . . 231

8.5 Improving Software Quality . . . . . 233

8.5.1 Techniques for Improving Software Quality . . . . . 234

8.6 Producer Protection . . . . . 235

8.7 References . . . . . 235

8.8 Further Reading . . . . . 237

8.9 Exercises . . . . . 237

## ... 9 COMPUTER CRIMES

9.1	Introduction . . . . .	240
9.2	History of Computer Crimes . . . . .	242
9.3	Computer Systems: Types of Attacks . . . . .	245
9.3.1	Penetration . . . . .	245
9.3.2	Denial of Service . . . . .	247
9.4	Motives of Attacks . . . . .	248
9.5	Costs and Social Consequences . . . . .	250
9.5.1	Lack of Cost Estimate Model for Cyberspace Attacks . . . . .	254
9.5.2	Social and Ethical Consequences . . . . .	258
9.6	References . . . . .	259
9.7	Further Reading . . . . .	260
9.8	Exercises . . . . .	261

## ... 10 NEW FRONTIERS FOR COMPUTER ETHICS ARTIFICIAL INTELLIGENCE, CYBERSPACE, AND VIRTUAL REALITY

10.1	Introduction . . . . .	264
10.2	Artificial Intelligence (AI) . . . . .	265
10.2.1	Advances in Artificial Intelligence . . . . .	266
10.2.2	Artificial Intelligence and Ethics . . . . .	268
10.2.3	The Future Role of Autonomous Agents . . . . .	271
10.3	Cyberspace . . . . .	272
10.4	Virtual Reality . . . . .	273
10.4.1	Ethics in Virtual Reality . . . . .	275
10.5	References . . . . .	278
10.6	Further Reading . . . . .	279
10.7	Exercises . . . . .	280

...1 1 CYBERSPACE AND CYBERETHICS

11.1 Introduction . . . . . 284

11.2 Cyberspace Safeguards . . . . . 285

11.2.1 Detecting Computer Attacks. . . . . 285

11.2.2 System Survivability . . . . . 289

11.3 Intellectual Property Rights in Cyberspace. . . . . 290

11.3.1 Copyrights . . . . . 294

11.3.2 Patents . . . . . 295

11.3.3 Trade Secrets . . . . . 296

11.3.4 Trademarks. . . . . 297

11.3.5 Personal Identity . . . . . 298

11.4 Regulating and Censoring Cyberspace . . . . . 299

11.5 The Social Value of Cyberspace . . . . . 303

11.6 Privacy in Cyberspace. . . . . 304

11.6.1 Privacy Protection . . . . . 306

11.7 Cyberspace Security . . . . . 306

11.7.1 Insecurity in the Basic Internet Infrastructure . . . . . 306

11.7.2 Server Security . . . . . 307

11.7.3 Security During Transmission . . . . . 308

11.8 Global Cyberethics . . . . . 311

11.9 Cyberspace Lingua Franca . . . . . 311

11.10 Global Cyber Culture. . . . . 314

11.11 Cyberethics and Social Realities in Cybercommunities. . 315

11.12 References. . . . . 318

11.13 Further Reading . . . . . 319

11.14 Exercises . . . . . 320

...1 2 COMPUTER NETWORKS AND ONLINE CRIMES

12.1 Introduction to Computer Networks . . . . . 323

12.1.1 Computer Network Models . . . . . 324

12.1.2 Computer Network Types . . . . . 325

12.2 Online Crimes . . . . . 327

12.2.1 Beware of Ways to Perpetuate Online Crimes. . . . . 329

<b>12.3</b>	<b>Defense Against Online Crimes . . . . .</b>	<b>332</b>
12.3.1	Prevention. . . . .	332
<b>12.4</b>	<b>Proven Security Protocols and Best Practices. . . . .</b>	<b>339</b>
12.4.1	Authentication . . . . .	340
12.4.2	Access Control . . . . .	340
12.4.3	Legislation . . . . .	341
12.4.4	Self-Regulation. . . . .	341
12.4.5	Detection . . . . .	341
12.4.6	Recovery. . . . .	342
<b>12.5</b>	<b>References . . . . .</b>	<b>342</b>

## ...1 3 COMPUTER CRIME INVESTIGATIONS- COMPUTER FORENSICS

<b>13.1</b>	<b>Introduction . . . . .</b>	<b>343</b>
<b>13.2</b>	<b>Digital Evidence . . . . .</b>	<b>344</b>
13.2.1	Looking for Digital Evidence. . . . .	345
13.2.2	Digital Evidence: Previewing and Acquisition . . . . .	345
<b>13.3</b>	<b>Preserving Evidence . . . . .</b>	<b>348</b>
<b>13.4</b>	<b>Analysis of Digital Evidence . . . . .</b>	<b>349</b>
13.4.1	Analyzing Data Files . . . . .	350
13.4.2	Analysis Based on Operating Systems. . . . .	352
13.4.3	Analysis Based on Digital Media . . . . .	353
<b>13.5</b>	<b>Relevance and Validity of Digital Evidence . . . . .</b>	<b>357</b>
<b>13.6</b>	<b>Writing Investigative Reports. . . . .</b>	<b>357</b>
<b>13.7</b>	<b>References . . . . .</b>	<b>358</b>

## ...1 4 BIOMETRICS

<b>14.1</b>	<b>Introduction and Definitions . . . . .</b>	<b>359</b>
14.1.1	Definitions . . . . .	360
<b>14.2</b>	<b>The Biometrics Authentication Process . . . . .</b>	<b>362</b>
<b>14.3</b>	<b>Biometric System Components. . . . .</b>	<b>363</b>
14.3.1	Data Acquisition. . . . .	363
14.3.2	Enrollments. . . . .	363

14.3.3 Signal Processing . . . . . 364

14.3.4 Decision Policy . . . . . 364

**14.4** Types of Biometric Technologies . . . . . 364

14.4.1 Finger Biometrics . . . . . 364

14.4.2 Hand Geometry . . . . . 368

14.4.3 Face Biometrics . . . . . 369

14.4.4 Voice Biometrics . . . . . 370

14.4.5 Handwriting Analysis . . . . . 371

14.4.6 Iris Biometrics . . . . . 371

14.4.7 Retina . . . . . 372

**14.5** The Future of Biometrics . . . . . 373

**14.6** References . . . . . 374

**... A** THE DIGITAL MILLENNIUM  
COPYRIGHT ACT . . . . . 377

**... B** THE FEDERAL FALSE CLAIMS ACT..... 391

**... C** PROJECTS . . . . . 417

**INDEX** . . . . . 421