Volume I

Section I
Fundamental Concepts and Theories

This section serves as a foundation for this exhaustive reference tool by addressing crucial theories essential to the fundamental understanding of cyber crime. Chapters found within these pages provide an excellent framework in which to position cyber crime within the field of information science and technology. Insight regarding the critical incorporation of global measures to prevent and protect against cyber crime are addressed, while crucial stumbling blocks of this field are explored. With 11 chapters comprising this foundational section, the reader can learn and chose from a compendium of expert research on the elemental theories underscoring the cyber crime discipline.

Chapter 1.1
Internet Crime: How Vulnerable Are You? Do Gender, Social Influence and Education Play a Role in vulnerability?

Tejaswini Herath, State University of New York, USA
H. R. Rao, State University of New York, USA
Shambhu Upadhyaya, State University of New York, USA

Chapter 1.2
Introduction to Basic Concepts and Considerations of Wireless Networking Security

Carlos F. Lerma, Universidad Autónoma de Tamaulipas, Mexico
Armando Vega, Universidad Autónoma de Tamaulipas, Mexico

Chapter 1.3
Cyber Identity Theft

Lynne D. Roberts, Curtin University of Technology, Australia

Chapter 1.4
Identity Theft Through the Web

Thomas M. Chen, Swansea University, UK
Chapter 1.5
How Safe Is Your Identity? Security Threats, Data Mining, and Digital Fingerprints/Footprints ....... 52
Bobbe Baggio, La Salle University, USA
Yoany Beldarrain, La Salle University, USA

Chapter 1.6
Antecedents of Online Privacy Protection Behavior: Towards an Integrative Model...................... 69
Anil Gurung, Neumann College, USA
Anurag Jain, Salem State College, USA

Chapter 1.7
Protection of Privacy on the Web ................................................................. 83
Thomas M. Chen, Swansea University, UK
Zhi (Judy) Fu, Motorola Labs, USA

Chapter 1.8
Online Privacy, Vulnerabilities, and Threats: A Manager’s Perspective...................................... 101
Hy Sockel, DIKW Management Group, USA
Louis K. Falk, University of Texas at Brownsville, USA

Chapter 1.9
Intrusion in the Sphere of Personal Communications.............................................................. 124
Judith Rauhofer, University of Central Lancashire, UK

Chapter 1.10
Data Mining and Privacy ......................................................................................... 146
Esma Aïmeur, Université de Montréal, Canada
Sébastien Gambs, Université de Montréal, Canada

Chapter 1.11
Data Mining and Privacy Protection........................................................................ 154
Armand Faganel, University of Primorska, Slovenia
Danijel Bratina, University of Primorska, Slovenia

Chapter 1.12
Deciphering the Hacker Underground: First Quantitative Insights ......................................... 175
Michael Bachmann, Texas Christian University, USA

Chapter 1.13
Globalization and Data Privacy: An Exploratory Study ....................................................... 195
Robert L. Totterdale, Robert Morris University, USA
Section II
Development and Design Methodologies

This section provides in-depth coverage of conceptual architecture frameworks to provide the reader with a comprehensive understanding of the emerging developments within the field of cyber crime. Research fundamentals imperative to the understanding of developmental processes within cyber crime are offered. From broad examinations to specific discussions on methodology, the research found within this section spans the discipline while offering detailed, specific discussions. From basic designs to abstract development, these chapters serve to expand the reaches of development and design technologies within the cyber crime prevention and protection fields. This section includes 9 contributions from researchers throughout the world on the topic of cyber crime.

Chapter 2.1
A Simulation Model of IS Security ................................................................. 214
Norman Pendegraft, University of Idaho, USA
Mark Rounds, University of Idaho, USA

Chapter 2.2
Security, Trust, and Privacy on Mobile Devices and Multimedia Applications ................. 228
Edgar R. Weippl, Secure Business Austria, Austria
Bernhard Riedl, Secure Business Austria, Austria

Chapter 2.3
A Multistage Framework to Defend Against Phishing Attacks ..................................... 245
Madhusudhanan Chandrasekaran, SUNY at Buffalo, USA
Shambhu Upadhyaya, State University of New York, USA

Chapter 2.4
A Framework for Privacy Assurance and Ubiquitous Knowledge Discovery in Health 2.0 Data Mashups ................................................................. 263
Jun Hu, University of Ottawa, Canada
Liam Peyton, University of Ottawa, Canada

Chapter 2.5
A Policy-Based Security Framework for Privacy-Enhancing Data Access and Usage Control in Grids ........................................................................ 284
Wolfgang Hommel, Leibniz Supercomputing Centre, Germany

Chapter 2.6
Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy ............................................................................. 300
Anna Tsiftsoglou, University of Athens, Greece
Chapter 2.7
An SOA-Based Architecture to Share Medical Data with Privacy Preservation

Mahmoud Barhamgi, Claude Bernard Lyon 1 University, France
Djamal Benslimane, Claude Bernard Lyon 1 University, France
Chirine Ghedira, Claude Bernard Lyon 1 University, France
Brahim Medjaged, University of Michigan-Dearborn, USA

Chapter 2.8
A Partial Optimization Approach for Privacy Preserving Frequent Itemset Mining

Shibnath Mukherjee, Yahoo! Research and Development, India
Aryya Gangopadhyay, University of Maryland Baltimore County, USA
Zhiyuan Chen, University of Maryland Baltimore County, USA

Chapter 2.9
A Methodology for UICC-Based Security Services in Pervasive Fixed Mobile Convergence Systems

Jaemin Park, Convergence WIBRO BU, KT (Korea Telecom), Republic of Korea

Chapter 2.10
An Analysis of Privacy and Security in the Zachman and Federal Enterprise Architecture Frameworks

Richard V. McCarthy, Quinnipiac University, USA

Chapter 2.11
A Game Theoretic Approach to Optimize Identity Exposure in Pervasive Computing Environments

Feng Zhu, The University of Alabama in Huntsville, USA
Sandra Carpenter, The University of Alabama in Huntsville, USA
Wei Zhu, Intergraph Co., USA
Matt W. Mutka, Michigan State University, USA

Chapter 2.12
Distributed Privacy Preserving Clustering via Homomorphic Secret Sharing and Its Application to (Vertically) Partitioned Spatio-Temporal Data

Can Yildizli, Sabanci University, Turkey
Thomas Brochmann Pedersen, Sabanci University, Turkey
Yucel Saygin, Sabanci University, Turkey
Erkay Savas, Sabanci University, Turkey
Albert Levi, Sabanci University, Turkey

Section III
Tools and Technologies

This section presents an extensive coverage of various tools and technologies available in the field of cyber crime that practitioners and academicians alike can utilize to develop different techniques to protect against hackers and security threats. These chapters enlighten readers about fundamental research
on the many methods used to facilitate and enhance the integration of this worldwide phenomenon by exploring the usage of artificial intelligence, meta-heuristics, security, and adaptive algorithms, to name a few. It is through these rigorously researched chapters that the reader is provided with countless examples of the up-and-coming tools and technologies emerging from the field of cyber crime. With 12 chapters, this section offers a broad treatment of some of the many tools and technologies within the cyber crime and IT community.

Chapter 3.1
Current Network Security Technology ................................................................. 417
Göran Pulkkis, Arcada Polytechnic, Finland
Kaj Grahn, Arcada Polytechnic, Finland
Peik Åström, Utimaco Safeware Oy, Finland

Chapter 3.2
Data Breach Disclosure: A Policy Analysis ......................................................... 430
Melissa Dark, Purdue University, USA

Chapter 3.3
Computer Hacking and the Techniques of Neutralization: An Empirical Assessment ......................................................... 457
Robert G. Morris, University of Texas at Dallas, USA

Chapter 3.4
Biometric Security in the E-World ................................................................. 474
Kunal Sharma, DOEACC Centre, India
A.J. Singh, H.P. University, India

Chapter 3.5
Biometric Controls and Privacy ................................................................. 524
Sean Lancaster, Miami University, USA
David C. Yen, Miami University, USA

Chapter 3.6
Dynamic Control Mechanisms for User Privacy Enhancement ........................................ 534
Amr Ali Eldin, Accenture, The Netherlands

Chapter 3.7
Privacy Regulation in the Metaverse ................................................................. 557
Ronald Leenes, Tilburg University, The Netherlands

Chapter 3.8
Efficient and Reliable Pseudonymous Authentication ........................................ 571
Giorgio Calandriello, Politecnico di Torino, Italy
Antonio Lioy, Politecnico di Torino, Italy

Chapter 3.9
Image Watermarking ........................................................................ 587
Nikos Tsirakis, University of Patras, Greece
Chapter 3.10
Memorizing Algorithm: Protecting User Privacy using Historical Information of Location-Based Services
Quynh Chi Truong, National University of Ho Chi Minh City, Vietnam
Anh Tuan Truong, National University of Ho Chi Minh City, Vietnam
Tran Khanh Dang, National University of Ho Chi Minh City, Vietnam

Volume II

Chapter 3.11
Detecting Shill Bidding in Online English Auctions
Jarrod Trevathan, James Cook University, Australia
Wayne Read, James Cook University, Australia

Chapter 3.12
Essential Mobile-Commerce Technology
Wen-Chen Hu, University of North Dakota, USA

Chapter 3.13
Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey
Emmanoul Magkos, Ionian University, Greece

Chapter 3.14
Do Privacy Statements Really Work? The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce
Hamid K. Nemati, The University of North Carolina, USA
Thomas Van Dyke, The University of North Carolina, USA

Section IV
Utilization and Application

This section discusses a variety of applications and opportunities available that can be considered by practitioners in developing viable and effective cyber crime prevention programs and processes. This section includes 16 chapters that review topics from Taiwan, Turkey, Romania, the United States, and many more countries, with dozens of institutions and cultures from around the world represented. A variety of chapters discuss cyber crime in a wide range of settings (crimes against women, information theft, cross-cultural theories of trust, etc.). Contributions included in this section provide excellent coverage of today’s IT community and how research into cyber crime is impacting the social fabric of our present-day global village.

Chapter 4.1
A Comparison of Cyber-Crime Definitions in India and the United States
Himanshu Maheshwari, University of South Florida, USA
H.S. Hyman, University of South Florida, USA
Manish Agrawal, University of South Florida, USA
Chapter 4.2
Cross Cultural Perceptions on Privacy in the United States, Vietnam, Indonesia, and Taiwan........ 727
  Andy Chiou, National Cheng Kung University, Taiwan
  Jeng-chung V. Chen, National Cheng Kung University, Taiwan
  Craig Bisset, National Cheng Kung University, Taiwan

Chapter 4.3
Cyber Victimization of Women and Cyber Laws in India.......................................................... 742
  Debarati Halder, Centre for Cyber Victim Counselling, India
  K. Jaishankar, Manonmaniam Sundaranar University, India

Chapter 4.4
Cyber Crime Against Women and Regulations in Australia......................................................... 757
  Debarati Halder, Centre for Cyber Victim Counselling, India
  K. Jaishankar, Manonmaniam Sundaranar University, India

Chapter 4.5
Cyber Laws for Preventing Cyber Crimes Against Women in Canada ........................................ 765
  Debarati Halder, Centre for Cyber Victim Counselling, India
  K. Jaishankar, Manonmaniam Sundaranar University, India

Chapter 4.6
Legal Treatment of Cyber Crimes Against Women in USA......................................................... 777
  Debarati Halder, Centre for Cyber Victim Counselling, India
  K. Jaishankar, Manonmaniam Sundaranar University, India

Chapter 4.7
Telecommunications Interception in Turkey: Rights to Privacy vs. Discourses of Security .......... 790
  Melike Akkaraca Köse, Marmara University, Turkey

Chapter 4.8
Online Privacy Protection in Japan: The Current Status and Practices ........................................ 814
  J. Michael Tarn, Western Michigan University, USA
  Naoki Hamamoto, Western Michigan University, USA

Chapter 4.9
Cross-Border Transfer of Personal Data: The Example of Romanian Legislation......................... 832
  Grigore-Octav Stan, Salans, Romania and King’s College London, UK
  Georgiana Ghitu, DLA Piper, Romania

Chapter 4.10
Digital Child Pornography: Offender or not Offender................................................................. 851
  Frank Y.W. Law, The University of Hong Kong, China
  K.P. Chow, The University of Hong Kong, China
  Pierre K.Y. Lai, The University of Hong Kong, China
  Hayson K.S. Tse, The University of Hong Kong, China
  Kenneth W.H. Tse, The University of Hong Kong, China
Chapter 4.11
Health Care Information Systems and the Risk of Privacy Issues for the Disabled

John Beswetherick, Capella University, USA

Chapter 4.12
Safeguarding the Privacy of Electronic Medical Records

Jingquan Li, Texas A&M University-San Antonio, USA
Michael J. Shaw, University of Illinois at Urbana-Champaign, USA

Chapter 4.13
Electronic Surveillance, Privacy and Enforcement of Intellectual Property Rights: A Digital Panopticon?

Pedro Pina, Polytechnic Institute of Coimbra, Portugal

Chapter 4.14
Secure Electronic Voting with Cryptography

Xunhua Wang, James Madison University, USA
Ralph Grove, James Madison University, USA
M. Hossain Heydari, James Madison University, USA

Chapter 4.15
U.S. Federal Data Mining Programs in the Context of the War on Terror: The Congress, Court, and Concerns for Privacy Protection

Shahid M. Shahidullah, Virginia State University, USA
Mokerom Hossain, Virginia State University, USA

Chapter 4.16
A Performance Study of Secure Data Mining on the Cell Processor

Hong Wang, Tohoku University, Japan
Hiroyuki Takizawa, Tohoku University, Japan
Hiroaki Kobayashi, Tohoku University, Japan

Chapter 4.17
Cryptographic and Steganographic Approaches to Ensure Multimedia Information Security and Privacy

Ming Yang, Jacksonville State University, USA
Monica Trifas, Jacksonville State University, USA
Guillermo Francia III, Jacksonville State University, USA
Lei Chen, Sam Houston State University, USA

Section V
Organizational and Social Implications

This section includes a wide range of research pertaining to the social and behavioral impact of cyber crime around the world. Chapters introducing this section critically analyze and discuss trends in information conservation and functional testing. Additional chapters included in this section look at
user and individual trust and ethical issues of surveillance techniques and privacy settings. Also investigating a concern within the field of cyber crime is research that discusses the effect of cyber crime on broadcast media. With 11 chapters, the discussions presented in this section offer research on the prevention of global cyber crime, as well as implementation of ethical considerations for all organizations.

Chapter 5.1
ICT Security Policy: Challenges and Potential Remedies ................................................................. 999

Lawan Ahmed Mohammed, King Fahd University of Petroleum and Minerals,
Saudi Arabia

Chapter 5.2
Definition, Typology and Patterns of Victimization ............................................................................. 1016

Debarati Halder; Centre for Cyber Victim Counselling, India
K. Jaishankar; Manonmaniam Sundaranar University, India

Chapter 5.3
Human Factors in Information Security and Privacy ........................................................................... 1043

Robert W. Proctor, Purdue University, USA
E. Eugene Schultz, High Tower Technologies, USA
Kim-Phuong L. Vu, California State University, USA

Chapter 5.4
Ensuring Users’ Rights to Privacy, Confidence and Reputation in the Online Learning Environment: What Should Instructors Do to Protect Their Students’ Privacy? ............................................. 1058

Louis B. Swartz, Robert Morris University, USA
Michele T. Cole, Robert Morris University, USA
David A. Lovejoy, Robert Morris University, USA

Chapter 5.5
Female and Male Hacker Conferences Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences ....................................................................................... 1075

Bernadette H. Schell, University of Ontario Institute of Technology, Canada
June Melnychuk, University of Ontario Institute of Technology, Canada

Chapter 5.6
Social/Ethical Issues in Predictive Insider Threat Monitoring ............................................................ 1100

Frank L. Gretzer, Pacific Northwest National Laboratory, USA
Deborah A. Frincke, Pacific Northwest National Laboratory, USA
Mariah Zabriskie, Pacific Northwest National Laboratory, USA

Chapter 5.7
The Human Attack in Linguistic Steganography ................................................................................... 1130

C. Orhan Orgun, University of California, Davis, USA
Vineeta Chand, University of California, Davis, USA
Chapter 5.8
How Much is Too Much? How Marketing Professionals can Avoid Violating Privacy Laws by Understanding the Privacy Principles
Nicholas P. Robinson, McGill University, Canada
Prescott C. Ensign, Telfer School of Management-University of Ottawa, Canada

Chapter 5.9
Audience Intelligence in Online Advertising
Bin Wang, Microsoft Corporation, China

Chapter 5.10
Effects of Individual Trust in Broadcast Media and the Internet on Privacy-Risking Uses of E-Health: An Expanded Analysis
E. Vance Wilson, Arizona State University, USA
David D. Dobrzykowski, Eastern Michigan University, USA
Joseph A. Cazier, Appalachian State University, USA

Chapter 5.11
Do You Know Where Your Data Is? A Study of the Effect of Enforcement Strategies on Privacy Policies
Ian Reay, University of Alberta, Canada
Patricia Beatty, University of Alberta, Canada
Scott Dick, University of Alberta, Canada
James Miller, University of Alberta, Canada

Chapter 5.12
Publicly Available Computers: An Investigation of Transactional Website Use through Computers in Public Locations
A.D. Rensel, Niagara University, USA
J.M. Abbas, The University of Oklahoma, USA
H.R. Rao, State University of New York at Buffalo, USA

Volume III

Section VI
Managerial Impact

This section presents contemporary coverage of the social implications of cyber crime, more specifically related to the corporate and managerial utilization of information sharing, privacy, and security technologies and applications, and how these technologies can be facilitated within organizations. Core ideas such as human resource management, supply chain forecasting, energy allocation, and software development technologies all pervade the section to give a clearer picture of the impact cyber crime has on management styles across different industries.
Chapter 6.1
Managing IS Security and Privacy ................................................................. 1246
Vasilios Katos, University of Portsmouth, UK

Chapter 6.2
Six Keys to Improving Wireless Security .................................................. 1255
Erik Graham, General Dynamics C4 Systems, USA
Paul John Steinbart, Arizona State University, USA

Chapter 6.3
A Game Theoretic Approach for Sensitive Information Sharing in Supply Chain.................. 1265
Xiaofeng Zhang, Hong Kong Baptist University, China
William Cheung, Hong Kong Baptist University, China
Zongwei Luo, The University of Hong Kong, China
Frank Tong, Technologies Research Center, Hong Kong, China

Chapter 6.4
An Analysis of Online Privacy Policies of Fortune 100 Companies ..................... 1276
Suhong Li, Bryant University, USA
Chen Zhang, Bryant University, USA

Chapter 6.5
Building and Management of Trust in Networked Information Systems ....................... 1292
István Mezgár, Hungarian Academy of Sciences, Hungary

Chapter 6.6
Regulation of Cybercafés in Nigeria .................................................................. 1305
Mercy Eyitemi, Delta State University, Nigeria

Chapter 6.7
Ross Wolf, University of Central Florida, USA
Ronnie Korosec, University of Central Florida, USA

Chapter 6.8
Responsibilities and Liabilities with Respect to Catastrophes .............................. 1328
C. Warren Axelrod, U.S. Trust, USA

Chapter 6.9
A Global Perspective of Laws and Regulations Dealing with Information Security and Privacy .............................................................................. 1349
B. Dawn Medlin, Appalachian State University, USA
Charlie C. Chen, Appalachian State University, USA
Chapter 6.10
A Case for Consumer Virtual Property ................................................................. 1364
Matt Hettche, Christopher Newport University, USA

Chapter 6.11
A Model-Based Privacy Compliance Checker ..................................................... 1379
Siani Pearson, Hewlett Packard Research Labs, UK
Damien Allison, Hewlett Packard Research Labs, UK

Chapter 6.12
Preventative Actions for Enhancing Online Protection and Privacy ..................... 1397
Steven Furnell, University of Plymouth, UK
Rossouw von Solms, Nelson Mandela Metropolitan University, South Africa
Andy Phippen, University of Plymouth, UK

Section VII
Critical Issues

This section contains 11 chapters giving a wide variety of perspectives on cyber crime and its implications. Such perspectives include the sense of security and trust, the personalization privacy paradox, and etiology and motives of cyber crime. The section also discusses taxonomical implications of the latest legal decisions as they pertain to cyber crime and security. Within the chapters, the reader is presented with an in-depth analysis of the most current and relevant issues within this growing field of study. Crucial questions are addressed and alternatives offered, such as genetic privacy and confidentiality within health and scientific research.

Chapter 7.1
The Sense of Security and Trust .............................................................................. 1409
Yuko Murayama, Iwate Prefectural University, Japan
Carl Hauser, Washington State University, USA
Natsuko Hikage, Iwate Prefectural University, Japan
Basabi Chakraborty, Iwate Prefectural University, Japan

Chapter 7.2
Examining an Individual’s Perceived Need for Privacy and Security: Construct and Scale Development ......................................................................................... 1419
Taner Pirim, Mississippi Center for Supercomputing Research, USA
Tabitha James, Virginia Polytechnic Institute, USA
Katherine Boswell, University of Louisiana – Monroe, USA
Brian Reithel, University of Mississippi, USA
Reza Barkhi, Virginia Polytechnic Institute, USA

Chapter 7.3
The Personalization Privacy Paradox: Mobile Customers’ Perceptions of Push-Based vs. Pull-Based Location Commerce ............................................................... 1431
Heng Xu, Pennsylvania State University, USA
John M. Carroll, Pennsylvania State University, USA
Mary Beth Rosson, Pennsylvania State University, USA
Chapter 7.4
Balancing the Public Policy Drivers in the Tension between Privacy and Security

John W. Bagby, The Pennsylvania State University, USA

Chapter 7.5
A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders

Bernadette H. Schell, University of Ontario Institute of Technology, Canada
Thomas J. Holt, The University of North Carolina at Charlotte, USA

Chapter 7.6
Etiology, Motives, and Crime Hubs

Debarati Halder, Centre for Cyber Victim Counselling, India
K. Jaishankar, Manonmaniam Sundaranar University, India

Chapter 7.7
The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?

Adam M. Bossler, Georgia Southern University, USA
George W. Burruss, University of Missouri-St. Louis, USA

Chapter 7.8
Between Hackers and White-Collar Offenders

Orly Turgeman-Goldschmidt, Bar-Ilan University, Israel

Chapter 7.9
What about the Balance between Law Enforcement and Data Protection?

Irene Portela, Polytechnic Institute of Cávado and Ave, Portugal
Maria Manuela Cruz-Cunha, Polytechnic Institute of Cávado and Ave, Portugal & University of Minho, Portugal

Chapter 7.10
A Taxonomic View of Consumer Online Privacy Legal Issues, Legislation, and Litigation

Angelena M. Secor, Western Michigan University, USA
J. Michael Tarn, Western Michigan University, USA

Chapter 7.11
Which Rights for Which Subjects? Genetic Confidentiality and Privacy in the Post-Genomic Era

Antoinette Rouvroy, European University Institute, Italy

Chapter 7.12
Provable Security for Outsourcing Database Operations

Sergei Evdokimov, Humboldt-Universität zu Berlin, Germany
Matthias Fischmann, Humboldt-Universität zu Berlin, Germany
Oliver Günther, Humboldt-Universität zu Berlin, Germany
Chapter 7.13
Minimising Collateral Damage: Privacy-Preserving Investigative Data Acquisition
Platform............................................................................................................................................. 1620

Zbigniew Kwecka, Edinburgh Napier University, UK
William J. Buchanan, Edinburgh Napier University, UK

Section VIII
Emerging Trends

This section highlights research potential within the field of cyber crime while exploring uncharted areas of study and future research directions. The section opens with a look at future trends in security, and what organizations can do to safeguard their employees’ information and their company data. Also of note among the final 9 chapters is a look at privacy in the age of social networks, and implications of said privacy towards a growing information age. In all, section 8 concludes the book well with suggestions towards where the field is heading and what to look forward to as data and information continue to grow and be threatened by hackers and security threats.

Chapter 8.1
Future Trends in Digital Security........................................................................................................ 1641

Daniel Viney, University of the Sunshine Coast, Australia

Chapter 8.2
Advances in Security and Privacy in Wireless Sensor Networks..................................................... 1654

Dulal C. Kar, Texas A&M University-Corpus Christi, USA
Hung L. Ngo, Texas A&M University-Corpus Christi, USA
Clifton J. Mulkey, Texas A&M University-Corpus Christi, USA
Geetha Sanapala, Texas A&M University-Corpus Christi, USA

Chapter 8.3
Advances in Privacy Preserving Record Linkage.................................................................................. 1682

Alexandros Karakasidis, University of Thessaly, Greece
Vassilios S. Verykios, University of Thessaly, Greece

Chapter 8.4
Emerging Security Issues in VANETs for E-Business........................................................................ 1695

S. S. Manvi, REVA Institute of Technology and Management, India
M. S. Kakkasageri, Basaveshwar Engineering College, India

Chapter 8.5
Cyber Security and Privacy in the Age of Social Networks............................................................... 1711

Babar Bhatti, MutualMind, Inc., USA

Chapter 8.6
Current Measures to Protect E-Consumers’ Privacy in Australia....................................................... 1728

Huong Ha, Monash University, Australia
Ken Coghill, Monash University, Australia
Elizabeth Ann Maharaj, Monash University, Australia
Chapter 8.7
Genetic Testing and Protection of Genetic Privacy: A Comparative Legal Analysis in Europe and Australia

Sergio Romeo-Malanda, University of Las Palmas de Gran Canaria, Spain
Dianne Nicol, University of Tasmania, Australia
Margaret Otlowski, University of Tasmania, Australia

1756

Chapter 8.8
Cryptography-Based Authentication for Protecting Cyber Systems

Xunhua Wang, James Madison University, USA
Hua Lin, University of Virginia, USA

1778

Chapter 8.9
Aspect-Oriented Programming and Aspect.NET as Security and Privacy Tool for Web and 3D Web Programming

Vladimir O. Safonov, St. Petersburg University, Russia

1797