Information Technology And Biometric Databases Eugenics And Other Threats To Disability Rights Journal Of Legal

This book presents the latest developments in biometrics technologies and reports on new approaches, methods, findings, and technologies developed or being developed by the research community and the industry. The book focuses

on introducing fundamental principles and concepts of key enabling technologies for biometric systems applied for both physical and cyber security. The authors disseminate recent research and developing efforts in this area, investigate related trends and challenges, and present case studies and examples such as fingerprint, face, iris, retina, keystroke dynamics, and voice applications . The authors also investigate the advances and future outcomes in research and development in biometric security systems. The book is applicable to students,

instructors, researchers, industry practitioners, and related government agencies staff. Each chapter is accompanied by a set of PowerPoint slides for use by instructors.

Databases, Biometrics, Information technology, Templates, Performance testing, Data security

This book considers biometric technology in a broad light, integrating the concept seamlessly into mainstream IT, while discussing the cultural attitudes and the societal impact of identity management. Features: summarizes the

material covered at the beginning of every chapter, and provides chapter-ending review questions and discussion points; reviews identity verification in nature, and early historical interest in anatomical measurement; provides an overview of biometric technology, presents a focus on biometric systems and true systems integration, examines the concept of identity management, and predicts future trends; investigates performance issues in biometric systems, the management and security of biometric data, and the impact of mobile devices on

biometrics technology; explains the equivalence of performance across operational nodes, introducing the APEX system; considers the legal, political and societal factors of biometric technology, in addition to user psychology and other human factors.

Fifty years ago, in 1984, George Orwell imagined a future in which privacy was demolished by a totalitarian state that used spies, video surveillance, historical revisionism, and control over the media to maintain its power. Those who worry about personal privacy and identity--especially in this

day of technologies that encroach upon these rights--still use Orwell's "Big Brother" language to discuss privacy issues. But the reality is that the age of a monolithic Big Brother is over. And yet the threats are perhaps even more likely to destroy the rights we've assumed were ours.Database Nation: The Death of Privacy in the 21st Century shows how, in these early years of the 21st century, advances in technology endanger our privacy in ways never before imagined. Direct marketers and retailers track our every purchase; surveillance cameras observe our

movements; mobile phones will soon report our location to those who want to track us; government eavesdroppers listen in on private communications; misused medical records turn our bodies and our histories against us; and linked databases assemble detailed consumer profiles used to predict and influence our behavior. Privacy--the most basic of our civil rights--is in grave peril.Simson Garfinkel--journalist, entrepreneur, and international authority on computer security--has devoted his career to testing new technologies and

warning about their implications. This newly revised update of the popular hardcover edition of Database Nation is his compelling account of how invasive technologies will affect our lives in the coming years. It's a timely, far-reaching, entertaining, and thought-provoking look at the serious threats to privacy facing us today. The book poses a disturbing question: how can we protect our basic rights to privacy, identity, and autonomy when technology is making invasion and control easier than ever before?Garfinkel's captivating blend of journalism,

storytelling, and futurism is a call to arms. It will frighten, entertain, and ultimately convince us that we must take action now to protect our privacy and identity before it's too late.

Computer Vision: Concepts, Methodologies, Tools, and Applications

The Practitioner's Guide to Biometrics

Australian and International Perspectives

for Surveillance and Security International Conferences, DTA / BSBT 2010, Held as Part of the Future Generation Information Technology Conference, FGIT

2010, Jeju Island, Korea, December 13-15, 2010. Proceedings

Biometric ID Management and Multimodal Communication

This book discusses recent advances and contemporary research in the field of cryptography, security, mathematics and statistics, and their applications in computing and information technology. Mainly focusing on mathematics and applications of mathematics in computer science and information technology, it includes contributions from eminent international scientists, researchers, and scholars. The book helps researchers update their knowledge

of cryptography, security, algebra, frame theory, optimizations, stochastic processes, compressive sensing, functional analysis, and complex variables.

This book is open access. This book undertakes a multifaceted and integrated examination of biometric identification, including the current state of the technology, how it is being used, the key ethical issues, and the implications for law and regulation. The five chapters examine the main forms of contemporary biometrics–fingerprint recognition, facial recognition and DNA identification– as well the integration of biometric data with other forms of personal data, analyses key ethical concepts in

play, including privacy, individual autonomy, collective responsibility, and joint ownership rights, and proposes a raft of principles to guide the regulation of biometrics in liberal democracies. Biometric identification technology is developing rapidly and being implemented more widely, along with other forms of information technology. As products, services and communication moves online, digital identity and security is becoming more important. Biometric identification facilitates this transition. Citizens now use biometrics to access a smartphone or obtain a passport; law enforcement agencies use biometrics in association with

CCTV to identify a terrorist in a crowd, or identify a suspect via their fingerprints or DNA; and companies use biometrics to identify their customers and employees. In some cases the use of biometrics is governed by law, in others the technology has developed and been implemented so quickly that, perhaps because it has been viewed as a valuable security enhancement, laws regulating its use have often not been updated to reflect new applications. However, the technology associated with biometrics raises significant ethical problems, including in relation to individual privacy, ownership of biometric data, dual use and, more generally, as is illustrated by the

increasing use of biometrics in authoritarian states such as China, the potential for unregulated biometrics to undermine fundamental principles of liberal democracy. Resolving these ethical problems is a vital step towards more effective regulation.

The development of technologies for the identi?cation of individuals has driven the interest and curiosity of many people. Spearheaded and inspired by the Bertillon coding system for the classi?cation of humans based on physical measurements, scientists and engineers have been trying to invent new devices and classi?cation systems to capture the human identity from its body

measurements. One of the main limitations of the precursors of today's biometrics, which is still present in the vast majority of the existing biometric systems, has been the need to keep the device in close contact with the subject to capture the biometric measurements. This clearly limits the applicability and convenience of biometric systems. This book presents an important step in addressing this limitation by describing a number of methodologies to capture meaningful biometric information from a distance. Most materials covered in this book have been presented at the International Summer School on Biometrics

which is held every year in Alghero, Italy and which has become a ?agship activity of the IAPR Technical Committee on Biometrics (IAPR TC4). The last four chapters of the book are derived from some of the best p- sentations by the participating students of the school. The educational value of this book is also highlighted by the number of proposed exercises and questions which will help the reader to better understand the proposed topics. Biometricsâ€"the use of physiological and behavioral characteristics for identification purposesâ€"has been promoted as a way to enhance security and identification efficiency. There are questions, however, about, among

other issues, the effectiveness of biometric security measures, usability, and the social impacts of biometric technologies. To address these and other important questions, the NRC was asked by DARPA, the DHS, and the CIA to undertake a comprehensive assessment of biometrics that examines current capabilities, future possibilities, and the role of the government in their developments. As a first step, a workshop was held at which a variety of views about biometric technologies and systems were presented. This report presents a summary of the workshopâ€™s five panels: scientific and technical challenges; measurement,

statistics, testing, and evaluation; legislative, policy, human, and cultural factors; scenarios and applications; and technical and policy aspects of information sharing. The results of this workshop coupled with other information will form the basis of the studyâ€™s final report.

Concepts, Methodologies, Tools, and Applications

Database Theory and Application, Bio-Science and Bio-Technology

Information Technology. Biometric Calibration, Augmentation and Fusion Data. Fusion Information Format

16th International Conference on Information Technology-New Generations (ITNG 2019)

Inventive Approaches for Technology Integration and Information Resources Management

Biometrics

Cloud technologies have revolutionized the way we store information and perform various computing tasks. With the rise of this new technology, the ability to secure information stored on the cloud becomes a concern. The Handbook of Research on Securing Cloud-Based Databases with Biometric Applications explores the latest innovations in promoting cloud security through human authentication techniques.

Exploring methods of access by identification, including the analysis of facial features, fingerprints, DNA, dental characteristics, and voice patterns, this publication is designed especially for IT professionals, academicians, and upper-level students seeking current research surrounding cloud security.

Many types of security technologies are currently in use, with biometrics being one of the latest and most cutting-edge forms that has been produced for mass application. Biometrics, while intriguing, is often broached with hesitation and

poor understanding. Adopting Biometric Technology: Challenges and Solutions advocates increased implementation of biometric technology areas of the world where it has been least accepted, particularly in the United States. This book looks at several specific applications of biometric technology, challenging issues that have obstructed the use of biometrics in security and offering realistic solutions for increasing its worldwide utilization. It is divided into three sections, with the first discussing societal barriers against the adoption of biometric

technology in security. The second section presents case studies of specific applications, such as e-passports and e-voting, that have already been implemented and could be expanded into regions where usage is low. The third section lays out a case for the general practicality and value that biometrics offers to relevant business sectors, including the benefits of implementing the currently controversial technology in place of the conventional forms of verification. While biometric technology has been poorly accepted and adopted in the

United States as well as other developed nations, it is already a popular tool in developing nations in Asia, Africa, and Eastern Europe. Adopting Biometric Technology examines the societal resistance hindering the broader usage of biometrics and provides practical solutions for overcoming those barriers while showing how its increased application would be overall advantageous.

This book constitutes the research papers presented at the Joint 2101 & 2102 International Conference on Biometric ID Management and Multimodal Communication.

BioID_MultiComm'09 is a joint International Conference organized cooperatively by COST Actions 2101 & 2102. COST 2101 Action is focused on 'Biometrics for Identity Documents and Smart Cards (BIDS)', while COST 2102 Action is entitled 'Cross-Modal Analysis of Verbal and Non-verbal Communication'. The aim of COST 2101 is to investigate novel technologies for unsupervised multimodal biometric authentication systems using a new generation of biometrics-enabled identity documents and smart cards. COST 2102 is devoted to

develop an advanced acoustical, perceptual and psychological analysis of verbal and non-verbal communication signals originating in spontaneous face-to-face interaction, in order to identify algorithms and automatic procedures capable of recognizing human emotional states.

The regulation of technology is an important and topical area of law, relevant to almost all aspects of society. Technology Law: Australian and International Perspectives presents a thorough exploration of the new legal challenges created by evolving

technologies, from the use of facial recognition technology in criminal investigations to the rise and regulation of cryptocurrencies. A well-written and fascinating introduction to technology law in Australia and internationally, Technology Law provides thorough coverage of the theoretical perspectives, legislation, cases and developing issues where technology and the law interact. The text covers data protection and privacy, healthcare technology, criminal justice technology, commercial transactions, cybercrime, social media and intellectual property, and canvasses the future of

technology and technology law. Written by leading experts in the field, Technology Law is an excellent resource for law students and legal professionals with an interest in the area.

A New Economy in Middle East and North Africa

Identity Verification in a Networked World

Challenges and Opportunities

Encyclopedia of Database Technologies and Applications

Handbook of Research on Securing Cloud-Based Databases with Biometric Applications

Information Technology.

Performance Testing of Biometric Template Protection

Schemes

Welcome to the proceedings of the 2010 International Conferences on Database Theory and Application (DTA 2010), and Bio-Science and Bio-Technology (BSBT 2010) – two of the partnering events of the Second International Mega-Conference on Future Generation Information Technology (FGIT 2010). DTA and BSBT bring together researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of

databases, data mining and biomedicine, including their links to computational sciences, mathematics and information technology. In total, 1,630 papers were submitted to FGIT 2010 from 30 countries, which includes 175 papers submitted to DTA/BSBT 2010. The submitted papers went through a rigorous reviewing process: 395 of the 1,630 papers were accepted for FGIT 2010, while 40 papers were accepted for DTA/BSBT 2010. Of the 40 papers 6 were selected for the

special FGIT 2010 volume published by Springer in the LNCS series. 31 papers are published in this volume, and 3 papers were withdrawn due to technical reasons. We would like to acknowledge the great effort of the DTA/BSBT 2010 International Advisory Boards and members of the International Program Committees, as well as all the organizations and individuals who supported the idea of publishing this volume of proceedings, including SERSC and Springer. Also,

the success of these two conferences would not have been possible without the huge support from our sponsors and the work of the Chairs and Organizing Committee.

Biometric Technologies and Verification Systems is organized into nine parts composed of 30 chapters, including an extensive glossary of biometric terms and acronyms. It discusses the current state-of-the-art in biometric verification/authentication, identification and system design principles. It also

provides a step-by-step discussion of how biometrics works; how biometric data in human beings can be collected and analyzed in a number of ways; how biometrics are currently being used as a method of personal identification in which people are recognized by their own unique corporal or behavioral characteristics; and how to create detailed menus for designing a biometric verification system. Only biometrics verification/au thentication is based on the identification of an

intrinsic part of a human being. Tokens, such as smart cards, magnetic stripe cards, and physical keys can be lost, stolen, or duplicated. Passwords can be forgotten, shared, or unintentionally observed by a third party. Forgotten passwords and lost "smart cards" are a nuisance for users and an expensive time-waster for system administrators. Biometric security solutions offer some unique advantages for identifying and verifying/ authenticating human beings over more

*traditional security methods. This book will serve to identify the various security applications biometrics can play a highly secure and specific role in. * Contains elements such as Sidebars, Tips, Notes and URL links * Heavily illustrated with over 150 illustrations, screen captures, and photographs * Details the various biometric technologies and how they work while providing a discussion of the economics, privacy issues and challenges of implementing biometric*

security solutions Biometric Systems provides practitioners with an overview of the principles and methods needed to build reliable biometric systems. It covers three main topics: key biometric technologies, design and management issues, and the performance evaluation of biometric systems for personal verification/identification. The four most widely used technologies are focused on - speech, fingerprint, iris and face recognition. Key features include: in-depth coverage of the technical and

practical obstacles which are often neglected by application developers and system integrators and which result in shortfalls between expected and actual performance; and protocols and benchmarks which will allow developers to compare performance and track system improvements. Healthcare sectors often deal with a large amount of data related to patients' care and hospital workforce management. Mistakes occur, and the impending results are disastrous for

individuals' personal identity information. However, an innovative and reliable way to safeguard the identity of individuals and provide protection of medical records from criminals is already in effect. Design and Implementation of Healthcare Biometric Systems provides innovative insights into medical identity theft and the benefits behind biometrics technologies that could be offered to protect medical records from hackers and malicious users. The content within

this publication represents the work of ASD screening systems, healthcare management, and patient rehabilitation. It is designed for educators, researchers, faculty members, industry practitioners, graduate students, and professionals working with healthcare services and covers topics centered on understanding the practical essence of next-generation healthcare biometrics systems and future research directions.

Hearing Before the

Committee on Armed Services, United States Senate, One Hundred Seventh Congress, First Session, October 25, 2001
Technological, Operational, and User-Related Factors
The Death of Privacy in the 21st Century
International Human Rights and Mental Disability Law
Joint COST 2101 and 2102 International Conference, BioID_MultiComm 2009, Madrid, Spain, September 16-18, 2009, Proceedings
When the Silenced are Heard

International Human Rights and

Mental Disability Law: When the Silenced are Heard draws attention to these issues in order to shed light on deplorable conditions that governments continue to ignore, and to invigorate the debate on a social policy issue that remains a low priority for most of the world's nations. Examining the mistreatment of persons with mental disabilities around the world, Michael Perlin identifies universal factors that contaminate mental disability law, including lack of comprehensive legislation and of independent counsel; inadequate care; poor or nonexistent community programming; and inhumane forensic systems. Using examples from Western and

Eastern Europe, South America, Africa and Asia, Perlin examines and summarizes the growing field of international mental health law, arguing that governmental inaction demeans human dignity, denies personal autonomy, and disregards the most authoritative and comprehensive prescription of human rights obligations. Biometrics is the most accurate form of identifiers and, when used properly, can greatly simplify life. However, biometrics raise new questions about personal privacy, surveillance, and the effects of government and corporate databases that register and hold fingerprint data and other biometric information. This book covers such

topics as ID cards, data theft, authentication, and digital rights management.

An insight into the biometric industry and the steps forsuccessful deployment Biometrics technologies verify identity through characteristicssuch as fingerprints, voices, and faces. By providing increasedsecurity and convenience, biometrics have begun to see widespreaddeployment in network, e-commerce, and retail applications. Thisbook provides in-depth analysis of biometrics as a solution forauthenticating employees and customers. Leading authority, SamirNanavati explores privacy, security, accuracy, system design, userperceptions, and

lessons learned in biometric deployments. He alsoassesses the real-world strengths and weaknesses of leadingbiometric technologies: finger-scan, iris-scan, facial-scan,voice-scan, and signature-scan. This accessible book is a necessarystep in understanding and implementing biometrics. Demystifies the complex world of optical networks for IT andbusiness managers Over the past few years, the cost of fiber optic networking hasdecreased, making it the best solution for providing virtuallyunlimited bandwidth for corporate LANs and WANs, metropolitannetworks, Internet access, and broadband to the home. The onlystrategic book

on optical networking technologies written from areal-world business perspective, Optical Networking demystifiescomplex fiber technologies for managers, and details the practicalbusiness benefits an optical network can offer. Debra Cameronexplores established and emerging markets for optical networks aswell as the enabling technologies, applications, networkarchitectures, key deployment issues, and cost considerations. Shealso provides in-depth case studies of optical networks now in usein the United States and abroad.

In this volume, thirteen authors from all points of the English-speaking world provide a tour of the

entwined labyrinths of technology and terrorism. They describe terrorism as an epistemological contact sport. With espionage, one can often deduce from a few pieces of the puzzle a plan's goals and its roots, its sources. But the goals of terrorists are both vague and hopelessly specific, while their means are restrained by rational, institutional thought. Thus, terrorists can be equally expected to flail out without any thought at all, as a child might exhibit in a temper tantrum, and to be hyper-rational, probing at the edges of the target for any weakness. Therefore, how terrorists use technology may not be determined by any particular level of technology but in the

probabilities for the target's expectation and defense regarding particular technologies. Fred Allen asks why Bin Laden and his organization were effective against the Russians but may have more trouble with free societies. Edward Tenner muses on the ironies of low-tech attacks and the dangers of over-reliance on high-tech sophistication. Such thoughts are tempered by direct and unreassuring reportage from the federal security front. Ann Larabee turns the telescope around, with a history showing that bomb-throwing is as American as apple pie. Toby Blyth takes us inside the theorists' backroom for a look at the ever-mutating ways, means, and motives

of war. It used to be about power, money, land, resources, or the ever-popular Pamir Knot "Great Game." Now it seems that globalization has coughed up groups of people, with little in common except for simultaneous feelings of helplessness and cultural superiority. Modern technology, which once seemed to hold only promise, now seems to harbor the potential for danger and destruction. The contributors to this volume are interested in the broader culture, and how terrorism affects that culture--including how people go about researching terrorism.

Biometric-Based Physical and Cybersecurity Systems

Information Technology and Applied Mathematics
Technology and Terrorism
The Role of the Department of Defense in Homeland Security
The Hidden (Dis)integration of Europe
Biometric Technology

Insecure transportation systems are costing our worldwide mobility-based economy as much as 6% of GDP annually. The effectiveness of security measures vary widely. In the United States, depending on the mode of transportation, it ranges from “medium effectiveness for airports to “low effectiveness for maritime, rail, transit, and intermodal activities. Situational awareness and interoperability are lacking as we try to deal with both

natural and man-made disasters. Regardless of the transport mode, improvements are essential if governments and corporations are to address security planning, response, and national preparedness. Transportation Security examines this problem in a comprehensive manner and addresses security-based technologies and solutions to minimize risk. * Covers air, sea, roadway, rail and public transport modes * Offers technological solutions for mobility based problems in planning, logistics and policy to improve security, combat terrorism and ensure national preparedness * Includes work of international experts & global examples related to transportation security

The fields of computer vision and

image processing are constantly evolving as new research and applications in these areas emerge. Staying abreast of the most up-to-date developments in this field is necessary in order to promote further research and apply these developments in real-world settings. Computer Vision: Concepts, Methodologies, Tools, and Applications is an innovative reference source for the latest academic material on development of computers for gaining understanding about videos and digital images. Highlighting a range of topics, such as computational models, machine learning, and image processing, this multi-volume book is ideally designed for academicians, technology professionals, students, and researchers interested in uncovering the

latest innovations in the field.

"Addresses the evolution of database management, technologies and applications along with the progress and endeavors of new research areas."--P. xiii.

This book constitutes the refereed proceedings of the 27th IFIP WG 11.3 International Conference on Data and Applications Security and Privacy, DBSec 2013, held in Newark, NJ, USA in July 2013. The 16 revised full and 6 short papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in topical sections on privacy, access control, cloud computing, data outsourcing, and mobile computing.

Middle East and North Africa Economic Monitor, October 2018

6th Chinese Conference, CCBR 2011, Beijing, China, December 3-4, 2011. Proceedings
Design and Implementation of Healthcare Biometric Systems
Biometric Recognition
Biometric Identification, Law and Ethics
Guide to Biometrics for Large-Scale Systems

Most biometric books are either extraordinarily technical for technophiles or extremely elementary for the lay person. Striking a balance between the two, Biometric Technology:

Authentication, Biocryptography, and Cloud-Based Architecture is ideal for business, IT, or security managers that are faced with the task of making purchasing, migration, o Biometric recognition--the automated recognition of individuals based on their behavioral and biological characteristic--is promoted as a way to help identify terrorists, provide better control of access

to physical facilities and financial accounts, and increase the efficiency of access to services and their utilization. Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics, and the personalization of social services, among other things. In spite of substantial effort, however, there remain unresolved questions about the effectiveness

and management of systems for biometric recognition, as well as the appropriateness and societal impact of their use. Moreover, the general public has been exposed to biometrics largely as high-technology gadgets in spy thrillers or as fear-instilling instruments of state or corporate surveillance in speculative fiction. Now, as biometric technologies appear poised for broader use, increased concerns about

national security and the tracking of individuals as they cross borders have caused passports, visas, and border-crossing records to be linked to biometric data. A focus on fighting insurgencies and terrorism has led to the military deployment of biometric tools to enable recognition of individuals as friend or foe. Commercially, finger-imaging sensors, whose cost and physical size have been reduced, now appear on many

laptop personal computers, handheld devices, mobile phones, and other consumer devices. Biometric Recognition: Challenges and Opportunities addresses the issues surrounding broader implementation of this technology, making two main points: first, biometric recognition systems are incredibly complex, and need to be addressed as such. Second, biometric recognition is an inherently probabilistic

endeavor. Consequently, even when the technology and the system in which it is embedded are behaving as designed, there is inevitable uncertainty and risk of error. This book elaborates on these themes in detail to provide policy makers, developers, and researchers a comprehensive assessment of biometric recognition that examines current capabilities, future possibilities, and the role of government in

technology and system development.
"After a sharp fall in 2017, economic growth in MENA is projected to rebound to 3.1 percent in 2018, thanks to the positive global outlook, oil prices stabilizing at relatively higher levels, stabilization policies and reforms, and recovery and reconstruction as conflicts recede. The outlook for MENA remains positive, and the growth rebound is expected to gain momentum over the

next two years, exceeding 3 percent in 2020. While stabilization policies have helped economies adjust in recent years, .a second phase of reforms is needed should be transformative if the region is to reach its potential and create jobs for hundred million young people who will enter the labor market in coming decades. In this report, we explore the role that public-private partnerships can play. not only in

providing an alternative source of financing but in helping change the role of the state from the main provider of employment to an enabler of private sector activity. Studies have shown that the gap between MENA economies and fast-growing ones is the performance of the services sector. The disruptive technology offers new opportunities for boosting private-sector-led growth through enhancement of high-tech jobs in the

services sector. The report argues that combining the region's fast-growing pool of university graduates and a heavy penetration of social media and smartphone, could serve as the foundation for a digital sector that could create much-needed private sector jobs for the youth over the next decade."

This 16th International Conference on Information Technology - New Generations (ITNG), continues an annual

event focusing on state of the art technologies pertaining to digital information and communications. The applications of advanced information technology to such domains as astronomy, biology, education, geosciences, security and health care are among topics of relevance to ITNG. Visionary ideas, theoretical and experimental results, as well as prototypes, designs, and tools that help the information

readily flow to the user are of special interest. Machine Learning, Robotics, High Performance Computing, and Innovative Methods of Computing are examples of related topics. The conference features keynote speakers, the best student award, poster award, service award, a technical open panel, and workshops/exhibits from industry, government and academia.

A Comparative Legal Analysis

Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric Systems
Adopting Biometric Technology
Guide to Biometric Reference Systems and Performance Evaluation
Handbook of Remote Biometrics
Data and Applications Security and Privacy XXVII
This book includes a selection of articles from the 2018 International Conference on Information Technology & Systems (ICITS 18), held on

January 10 – 12, 2018, at the Universidad Estatal Península de Santa Elena, Libertad City, Ecuador. ICIST is a global forum for researchers and practitioners to present and discuss recent findings and innovations, current trends, lessons learned and the challenges of modern information technology and systems research, together with their technological development and applications. The main topics covered include information and knowledge management; organizational models and information systems; software and systems modeling; software systems, architectures, applications and tools; multimedia

systems and applications; computer networks, mobility and pervasive systems; intelligent and decision support systems; big data analytics and applications; human–computer interaction; ethics, computers & security; health informatics; and information technologies in education.

This book discusses all critical privacy and data protection aspects of biometric systems from a legal perspective. It contains a systematic and complete analysis of the many issues raised by these systems based on examples worldwide and provides several recommendations for a

transnational regulatory framework. An appropriate legal framework is in most countries not yet in place. Biometric systems use facial images, fingerprints, iris and/or voice in an automated way to identify or to verify (identity) claims of persons. The treatise which has an interdisciplinary approach starts with explaining the functioning of biometric systems in general terms for non-specialists. It continues with a description of the legal nature of biometric data and makes a comparison with DNA and biological material and the regulation thereof. After describing the risks, the work

further reviews the opinions of data protection authorities in relation to biometric systems and current and future (EU) law. A detailed legal comparative analysis is made of the situation in Belgium, France and the Netherlands. The author concludes with an evaluation of the proportionality principle and the application of data protection law to biometric data processing operations, mainly in the private sector. Pleading for more safeguards in legislation, the author makes several suggestions for a regulatory framework aiming at reducing the risks of biometric systems. They include

limitations to the collection and storage of biometric data as well as technical measures, which could influence the proportionality of the processing. The text is supported by several figures and tables providing a summary of particular points of the discussion. The book also uses the 2012 biometric vocabulary adopted by ISO and contains an extensive bibliography and literature sources.

Most biometric books are either extraordinarily technical for technophiles or extremely elementary for the lay person. Striking a balance between the two, Biometric Technology:

Authentication, Biocryptography, and Cloud-Based Architecture is ideal for business, IT, or security managers that are faced with the task of making purchasing, migration, or adoption decisions. It brings biometrics down to an understandable level, so that you can immediately begin to implement the concepts discussed. Exploring the technological and social implications of widespread biometric use, the book considers the science and technology behind biometrics as well as how it can be made more affordable for small and medium-sized business. It also presents the results of recent research on how the principles of

cryptography can make biometrics more secure. Covering biometric technologies in the cloud, including security and privacy concerns, the book includes a chapter that serves as a "how-to manual" on procuring and deploying any type of biometric system. It also includes specific examples and case studies of actual biometric deployments of localized and national implementations in the U.S. and other countries. The book provides readers with a technical background on the various biometric technologies and how they work. Examining optimal application in various settings and

their respective strengths and weaknesses, it considers ease of use, false positives and negatives, and privacy and security issues. It also covers emerging applications such as biocryptography. Although the text can be understood by just about anybody, it is an ideal resource for corporate-level executives who are considering implementing biometric technologies in their organizations.

This open access book explores how biometric data is increasingly flowing across borders in order to limit, control and contain the mobility of selected people, namely criminalized populations.

It introduces the concept of bio-bordering, using it to capture reverse patterns of bordering and ordering practices linked to transnational biometric data exchange regimes. The concept is useful to reconstruct how the territorial foundations of national state autonomy are partially reclaimed and, at the same time, partially purposefully suspended. The book focuses on the Prüm system, which facilitates the mandatory exchange of forensic DNA data amongst EU Member States. The Prüm system is an underexplored phenomenon, representing diverse instances of bio-bordering and providing a

complex picture of the hidden (dis)integration of Europe. Particular legal, scientific, technical and political dimensions related to the governance and uses of biometric technologies in Germany, the Netherlands, Poland, Portugal and the United Kingdom are specifically explored to demonstrate both similar and distinct patterns.

Technology Law

Authentication, Biocryptography, and Cloud-Based Architecture

Biometric Systems

Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)

ICITAM 2017

Modes of Bio-Bordering

Biometrics has moved from using fingerprints to using many methods of assessing human physical and behavioral traits. This guide introduces a new performance evaluation framework designed to offer full coverage of performance evaluation of biometric systems. Today□s management world continually relies on technological efficiency to function and perform at a high standard. As technology becomes a greater part in many fields, understanding and managing this factor is integral for organizations. Inventive Approaches for Technology

Integration and Information Resources Management provides an overview and analysis of knowledge management in sustainability, emergency preparedness, and IT, among other fields integral to the modern technological era. By providing a foundation for innovative practices in using technology and information resources, this publication is essential for practitioners and professionals, as well as undergraduate/graduate students and academicians.

This book constitutes the refereed proceedings of the 6th Chinese Conference on Biometric Recognition, CCBR 2011, held in Beijing, China in December 2011. The 35 revised full papers were

carefully reviewed and selected from 71 submissions. The papers are organized in topical sections on problems in face; iris; hand biometrics; speaker; handwriting; gait; behavioral and soft biometrics; and security.

Data processing, Biometrics, Calibration, Human body, Identification methods, Information exchange, Data merging, Algorithms, Data representation, Data organization, Databases, Statistics

Challenges and Solutions

Database Nation

Emerging Trends in Information Technology

Transportation Security

Report (to Accompany S. 2537).

27th Annual IFIP WG 11.3

Conference, DBSec 2013, Newark, NJ, USA, July 15-17, 2013, Proceedings

Security and Access Control Using Biometric Technologies presents an introduction to biometrics or the study of recognizing individuals based on their unique physical or behavioral traits, as they relate to computer security. The book begins with the basics of biometric technologies and discusses how and why biometric systems are emerging in information security. An emphasis is directed towards authentication, authorization, identification, and access control.

Topics covered include security and management required to protect valuable computer and network resources and assets, and methods of providing control over access and security for computers and networks. Written for a broad level of readers, this book applies to information system and information technology students, as well as network managers, security administrators and other practitioners. Oriented towards the practical application of biometrics in the real world, Security and Access Control Using Biometric Technologies provides the reader with a

realistic view of the use of biometrics in the ever-changing industry of information security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Biometric Technologies and Verification Systems

Department of Homeland Security Appropriations Bill, 2005

Security and Access Control Using Biometric Technologies

Technology, Design and Performance Evaluation

Privacy and Data Protection Issues of Biometric Applications