Privacy And Data Protection Issues Of Biometric Applications A Comparative Legal Analysis Law Governance And Technology Series

If you ally dependence such a referred **privacy and data protection issues of biometric applications a comparative legal analysis law governance and technology series** books that will manage to pay for you worth, acquire the certainly best seller from us currently from several preferred authors. If you desire to witty books, lots of novels, tale, jokes, and more fictions collections are afterward launched, from best seller to one of the most current released.

You may not be perplexed to enjoy all ebook collections privacy and data protection issues of biometric applications a comparative legal analysis law governance and technology series that we will totally offer. It is not concerning the costs. Its more or less what you compulsion currently. This privacy and data protection issues of biometric applications a comparative legal analysis law governance and technology series, as one of the most vigorous sellers here will enormously be accompanied by the best options to review.

Handbook of Digital Face Manipulation and Detection - Christian Rathgeb 2022-01-31 This open access book provides the first comprehensive collection of studies dealing with the hot topic of digital face manipulation such as DeepFakes, Face Morphing, or Reenactment. It combines the research fields of biometrics and media forensics including contributions from academia and industry. Appealing to a broad readership, introductory chapters provide a comprehensive overview of the topic, which address readers wishing to gain a brief overview of the state-of-the-art. Subsequent chapters, which delve deeper into various research challenges, are oriented towards advanced readers. Moreover, the book provides a good starting point for young researchers as well as a reference guide pointing at further literature. Hence, the primary readership is academic institutions and industry currently involved in digital face manipulation and detection. The book could easily be used as a recommended text for courses in image processing, machine learning, media forensics, biometrics, and the general security area.

Biometrics For Dummies - Peter H. Gregory 2009-02-25 What is biometrics? Whether you're just curious about how biometrics can benefit society or you need to learn how to integrate biometrics with an existing security system in your organization, Biometrics For Dummies can help. Here's a friendly introduction to biometrics — the science of identifying humans based on unique physical characteristics. With the government's use of biometrics — for example, biometric passport readers — and application of the technology for law enforcement, biometrics is growing more popular among security experts. Biometrics For Dummies explains biometric technology, explores biometrics policy and privacy issues with biometrics, and takes a look at where the science is heading. You'll

discover: How pattern recognition and fingerprint recognition are used The many vulnerabilities of biometric systems and how to guard against them How various countries are handling the privacy issues and what can be done to protect citizens' privacy How a scan of the palm, veins in the hand, and sonar imagery establish identity What it takes to fully authenticate a signature How gait, speech, linguistic analysis, and other types of biometric identification come into play The criteria for setting up an implementation plan How to use authentication, authorization, and access principles Written by a pair of security experts, Biometrics For Dummies gives you the basics in an easy-to-understand format that doesn't scrimp on substance. You'll get up to speed and enjoy getting there!

The GDPR Challenge - Amie Taal 2021-11-18

Consent is necessary for collecting, processing and transferring Personal Identifiable Information (PII) and sensitive personal data. But to what extent? What are the limitations and restricts to avoid penalties under The General Data Protection Regulation 2018 (GDPR) rules, which may be up to 4% of annual global turnover or €20 million (whichever is higher), enforcements and sanctions? Under GDPR Article 51, each EU Member State shall maintain an independent public authority to be responsible for monitoring the application of this regulation to protect the fundamental rights of data subjects (Supervisory Authority). The Supervisory Authority has powers to issue warnings, conduct audits, recommend remediation, order erasure of data and suspend data transfers to a third country. GDPR has changed the way data is used, accessed and stored. It's reach extends well beyond the European Union and is the basis of other data privacy laws around the world. This book provides a review and guidance on implementing and compliance of GDPR while taking

advantage of technology innovations and supported by real-life examples. The book shows the wide scope of applications to protect data privacy while taking advantage of processes and techniques in various fields such as eDiscovery, Cyber Insurance, Virtual-based Intelligence, Information Security, Cyber Security, Information Governance, Blockchain and Biometric technologies and techniques.

Biometric Identification, Law and Ethics - Marcus Smith 2021-12-11

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.

Biometric-Based Physical and Cybersecurity Systems - Mohammad S. Obaidat 2018-10-24

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.

Biometric and Auditing Issues Addressed in a Throughput Model - Waymond Rodgers 2011-12-01

This book proposes a Throughput Model that draws

from computer science, economic and psychology literatures to model perceptual and judgmental processes whereby biometrics might be used to reduce risks to a company's internal control. The book also discusses challenges in employing biometric technology and pinpoints avenues for future research. Biometrics is the examination of measurable biological characteristics. In organizational security, biometrics refers to tools that rely on measurable physical and behavioral characteristics that can be automatically checked. The Throughput Modeling process enables organizations to employ trust systems in assisting transactions that are motivated by ethical considerations. Auditing systems are by far based on trust. Concepts of ethics and trust are aided by the employment of biometrics technology, which enhances the transactions between individuals and organizations in an internal control environment. Issues pertaining to sustainability are also examined with the assistance of the Throughput Model. Finally, this book examines the potential use of an internal control biometrics system to lessen threats to identification and verification procedures. This book proposes an "Throughput Model framework" that considers both exposure and information risks as fundamental factors in classifying applications and organizational processes that might be candidates for the type of internal control biometrics system that biometrics can offer.

Biometrics, Surveillance and the Law - Sara M. Smyth 2019-03-04

The use of biometric identification systems is rapidly increasing across the world, owing to their potential to combat terrorism, fraud, corruption and other illegal activities. However, critics of the technology complain that the creation of an extensive central register of personal information controlled by the government will increase

opportunities for the state to abuse citizens. There is also concern about the extent to which data about an individual is recorded and kept. This book reviews some of the most current and complex legal and ethical issues relating to the use of biometrics. Beginning with an overview of biometric systems, the book goes on to examine some of the theoretical underpinnings of the surveillance state, questioning whether these conceptual approaches are still relevant, particularly the integration of ubiquitous surveillance systems and devices. The book also analyses the implementation of the world's largest biometric database, Aadhaar, in detail. Additionally, the identification of individuals at border checkpoints in the United States, Australia and the EU is explored, as well as the legal and ethical debates surrounding the use of biometrics regarding: the war on terror and the current refugee crisis; violations of international human rights law principles; and mobility and privacy rights. The book concludes by addressing the collection, use and disclosure of personal information by private-sector entities such as Axciom and Facebook, and government use of these tools to profile individuals. By examining the major legal and ethical issues surrounding the debate on this rapidly emerging technology, this book will appeal to students and scholars of law, criminology and surveillance studies, as well as law enforcement and criminal law practitioners.

Handbook of Research on Securing Cloud-Based Databases with Biometric Applications - Deka, Ganesh Chandra 2014-10-31

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.

European Data Protection: Coming of Age - Serge Gutwirth 2012-11-26

On 25 January 2012, the European Commission presented its long awaited new "Data protection package". With this proposal for a drastic revision of the data protection framework in Europe, it is fair to say that we are witnessing a rebirth of European data protection, and perhaps, its passage from an impulsive youth to a more mature state. Technology advances rapidly and mobile devices are significantly changing the landscape. Increasingly, we carry powerful, connected, devices, whose location and activities can be monitored by various stakeholders. Very powerful social network sites emerged in the first half of last decade, processing personal data of many millions of users. Updating the regulatory network was imminent and the presentation of the new package will initiate a period of intense debate in which the proposals will be thoroughly commented upon and criticized, and numerous amendments will undoubtedly be proposed. This volume brings together some 19 chapters offering conceptual analyses, highlighting issues, proposing solutions, and discussing practices regarding privacy and data protection. In the first part of the book, conceptual analyses of concepts such as privacy and anonymity are provided. The second section focuses on the contrasted positions of digital natives and ageing users in the information society. The third section provides four chapters on privacy by design, including

discussions on roadmapping and concrete techniques. The fourth section is devoted to surveillance and profiling, with illustrations from the domain of smart metering, self-surveillance and the benefits and risks of profiling. The book concludes with case studies pertaining to communicating privacy in organisations, the fate of a data protection supervisor in one of the EU member states and data protection in social network sites and online media. This volume brings together some 19 chapters offering conceptual analyses, highlighting issues, proposing solutions, and discussing practices regarding privacy and data protection. In the first part of the book, conceptual analyses of concepts such as privacy and anonymity are provided. The second section focuses on the contrasted positions of digital natives and ageing users in the information society. The third section provides four chapters on privacy by design, including discussions on roadmapping and concrete techniques. The fourth section is devoted to surveillance and profiling, with illustrations from the domain of smart metering, self-surveillance and the benefits and risks of profiling. The book concludes with case studies pertaining to communicating privacy in organisations, the fate of a data protection supervisor in one of the EU member states and data protection in social network sites and online media.

Biometrics in a Data Driven World - Sinjini Mitra 2016-12-01

Biometrics in a Data Driven World: Trends, Technologies, and Challenges aims to inform readers about the modern applications of biometrics in the context of a data-driven society, to familiarize them with the rich history of biometrics, and to provide them with a glimpse into the future of biometrics. The first section of the book discusses the fundamentals of biometrics and provides an overview of common biometric modalities, namely face, fingerprints, iris,

and voice. It also discusses the history of the field, and provides an overview of emerging trends and opportunities. The second section of the book introduces readers to a wide range of biometric applications. The next part of the book is dedicated to the discussion of case studies of biometric modalities currently used on mobile applications. As smartphones and tablet computers are rapidly becoming the dominant consumer computer platforms, biometrics-based authentication is emerging as an integral part of protecting mobile devices against unauthorized access, while enabling new and highly popular applications, such as secure online payment authorization. The book concludes with a discussion of future trends and opportunities in the field of biometrics, which will pave the way for advancing research in the area of biometrics, and for the deployment of biometric technologies in real-world applications. The book is designed for individuals interested in exploring the contemporary applications of biometrics, from students to researchers and practitioners working in this field. Both undergraduate and graduate students enrolled in college-level security courses will also find this book to be an especially useful companion.

Handbook of Research on Cyber Law, Data Protection, and Privacy - Dewani, Nisha Dhanraj 2022-04-22

The advancement of information and communication technology has led to a multi-dimensional impact in the areas of law, regulation, and governance. Many countries have declared data protection a fundamental right and established reforms of data protection law aimed at modernizing the global regulatory framework. Due to these advancements in policy, the legal domain has to face many challenges at a rapid pace making it essential to study and discuss policies and laws that regulate and monitor

these activities and anticipate new laws that should be implemented in order to protect users. The Handbook of Research on Cyber Law, Data Protection, and Privacy focuses acutely on the complex relationships of technology and law both in terms of substantive legal responses to legal, social, and ethical issues arising in connection with growing public engagement with technology and the procedural impacts and transformative potential of technology on traditional and emerging forms of dispute resolution. Covering a range of topics such as artificial intelligence, data protection, and social media, this major reference work is ideal for government officials, policymakers, industry professionals, academicians, scholars, researchers, practitioners, instructors, and students.

Handbook of Computer Networks and Cyber Security - Brij B. Gupta 2019-12-31

This handbook introduces the basic principles and fundamentals of cyber security towards establishing an understanding of how to protect computers from hackers and adversaries. The highly informative subject matter of this handbook, includes various concepts, models, and terminologies along with examples and illustrations to demonstrate substantial technical details of the field. It motivates the readers to exercise better protection and defense mechanisms to deal with attackers and mitigate the situation. This handbook also outlines some of the exciting areas of future research where the existing approaches can be implemented. Exponential increase in the use of computers as a means of storing and retrieving security-intensive information, requires placement of adequate security measures to safeguard the entire computing and communication scenario. With the advent of Internet and its underlying technologies, information security aspects

are becoming a prime concern towards protecting the networks and the cyber ecosystem from variety of threats, which is illustrated in this handbook. This handbook primarily targets professionals in security, privacy and trust to use and improve the reliability of businesses in a distributed manner, as well as computer scientists and software developers, who are seeking to carry out research and develop software in information and cyber security. Researchers and advanced-level students in computer science will also benefit from this reference.

Deep Learning Approaches to Cloud Security - Pramod Singh Rathore 2021-12-29 DEEP LEARNING APPROACHES TO CLOUD SECURITY Covering one of the most important subjects to our society today, cloud security, this editorial team delves into solutions taken from evolving deep learning approaches, solutions allowing computers to learn from experience and understand the world in terms of a hierarchy of concepts, with each concept defined through its relation to simpler concepts. Deep learning is the fastest growing field in computer science. Deep learning algorithms and techniques are found to be useful in different areas like automatic machine translation, automatic handwriting generation, visual recognition, fraud detection, and detecting developmental delay in children. However, applying deep learning techniques or algorithms successfully in these areas needs a concerted effort, fostering integrative research between experts ranging from diverse disciplines from data science to visualization. This book provides state of the art approaches of deep learning in these areas, including areas of detection and prediction, as well as future framework development, building service systems and analytical aspects. In all these topics, deep learning approaches, such as artificial neural networks, fuzzy logic, genetic algorithms, and hybrid mechanisms are used. This book is intended for

dealing with modeling and performance prediction of the efficient cloud security systems, thereby bringing a newer dimension to this rapidly evolving field. This groundbreaking new volume presents these topics and trends of deep learning, bridging the research gap, and presenting solutions to the challenges facing the engineer or scientist every day in this area. Whether for the veteran engineer or the student, this is a must-have for any library. Deep Learning Approaches to Cloud Security: Is the first volume of its kind to go in-depth on the newest trends and innovations in cloud security through the use of deep learning approaches Covers these important new innovations, such as AI, data mining, and other evolving computing technologies in relation to cloud security Is a useful reference for the veteran computer scientist or engineer working in this area or an engineer new to the area, or a student in this area Discusses not just the practical applications of these technologies, but also the broader concepts and theory behind how these deep learning tools are vital not just to cloud security, but society as a whole Audience: Computer scientists, scientists and engineers working with information technology, design, network security, and manufacturing, researchers in computers, electronics, and electrical and network security, integrated domain, and data analytics, and students in these areas

Information Privacy Law - Daniel J. Solove 2022-10-27 The Seventh Edition of Information Privacy Law has been revised to include the California Consumer Privacy Act, the GDPR, Carpenter, state biometric data laws, and many other new developments. A clear, comprehensive, and cutting-edge introduction to the field of information privacy law, Information Privacy Law contains the latest cases and materials exploring issues of emerging technology and information privacy, and the

extensive background information and authorial guidance provide clear and concise introductions to various areas of law. New to the Seventh Edition: Additional Coverage or updates to: California Consumer Privacy Act Carpenter v. United States General Data Protection Regulation State biometric data laws New FTC enforcement actions, including Facebook Professors and students will benefit from: Extensive coverage of FTC privacy enforcement, HIPAA and HHS enforcement, standing in privacy lawsuits, among other topics. Chapters devoted exclusively to data security, national security, employment privacy, and education privacy. Sections on government surveillance and freedom to explore ideas. Extensive coverage of the NSA and the Snowden revelations and the ensuing regulation. Engaging approach to complicated laws and regulations such as HIPAA, FCRA, ECPA, GDPR, and CCPA.

Security and Access Control Using Biometric Technologies - Robert Newman 2009-09-03 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.

Handbook of Biometric Anti-Spoofing - Sébastien Marcel 2014-07-17

Presenting the first definitive study of the subject, this Handbook of Biometric Anti-Spoofing reviews the state of the art in covert attacks against biometric systems and in deriving countermeasures to these attacks. Topics and features: provides a detailed introduction to the field of biometric anti-spoofing and a thorough review of the associated literature; examines spoofing attacks against five biometric modalities, namely, fingerprints, face, iris, speaker and gait; discusses anti-spoofing measures for multi-model biometric systems; reviews evaluation methodologies, international standards and legal and ethical issues; describes current challenges and suggests directions for future research; presents the latest work from a global selection of experts in the field, including members of the TABULA RASA project.

Data Protection and Privacy - Ronald Leenes 2018-12-13

The subjects of Privacy and Data Protection are more relevant than ever, and especially since 25 May 2018, when the European General Data Protection Regulation became enforceable. This volume brings together papers that offer conceptual analyses, highlight issues, propose solutions, and discuss practices regarding privacy and data protection. It is one of the results of the eleventh annual International Conference on Computers, Privacy, and Data Protection, CPDP 2018, held in Brussels in January 2018. The

book explores the following topics: biometrics and data protection in criminal justice processing, privacy, discrimination and platforms for men who have sex with men, mitigation through data protection instruments of unfair inequalities as a result of machine learning, privacy and human-robot interaction in robotized healthcare, privacy-by-design, personal data protection of deceased data subjects, large-scale face databases and the GDPR, the new Europol regulation, rethinking trust in the Internet of Things, fines under the GDPR, data analytics and the GDPR, and the essence of the right to the protection of personal data. This interdisciplinary book was written while the reality of the General Data Protection Regulation 2016/679 was becoming clear. It discusses open issues and daring and prospective approaches. It will serve as an insightful resource for readers with an interest in computers, privacy and data protection.

Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles - Olga Mironenko Enerstvedt 2017-09-18

This book sheds light on aviation security, considering both technologies and legal principles. It considers the protection of individuals in particular their rights to privacy and data protection and raises aspects of international law, human rights and data security, among other relevant topics. Technologies and practices which arise in this volume include body scanners, camera surveillance, biometrics, profiling, behaviour analysis, and the transfer of air passenger personal data from airlines to state authorities. Readers are invited to explore questions such as: What right to privacy and data protection do air passengers have? How can air passenger rights be safeguarded, whilst also dealing appropriately with security threats at airports and in airplanes? Chapters explore these dilemmas and examine approaches to aviation security

which may be transferred to other areas of transport or management of public spaces, thus making the issues dealt with here of paramou nt importance to privacy and human rights more broadly. The work presented here reveals current processes and tendencies in aviation security, such as globalization, harmonization of regulation, modernization of existing data privacy regulation, mechanisms of self-regulation, the growing use of Privacy by Design, and improving passenger experience. This book makes an important contribution to the debate on what can be considered proportionate security, taking into account concerns of privacy and related human rights including the right to health, freedom of movement, equal treatment and non-discrimination, freedom of thought, conscience and religion, and the rights of the child. It will be of interest to graduates and researchers in areas of human rights, international law, data security and related areas of law or information science and technology. I think it will also be of interest to other categories (please see e.g. what the reviewers have written) "I think that the book would be of great appeal for airports managing bodies, regulators, Civil Aviation Authorities, Data Protection Authorities, air carriers, any kind of security companies, European Commission Transport Directorate, European Air Safety Agency (EASA), security equipment producers, security agencies like the US TSA, university researchers and teachers." "Lawyers (aviation, privacy and IT lawyers), security experts, aviation experts (security managers of airports, managers and officers from ANSPs and National Aviation Authorities), decision makers, policy makers (EASA, EUROCONTROL, EU commission)"

The Future of Identity in the Information Society - Simone Fischer-Hübner 2010-08-25

The increasing diversity of

Infonnation Communication Technologies and their equally diverse range of uses in personal, professional and official capacities raise challenging questions of identity in a variety of contexts. Each communication exchange contains an identifier which may, or may not, be intended by the parties involved. What constitutes an identity, how do new technologies affect identity, how do we manage identities in a globally networked infonnation society? th th From the 6 to the 10 August 2007, IFIP (International Federation for Infonnation Processing) working groups 9. 2 (Social Accountability), 9. 6/11. 7 (IT rd Misuse and the Law) and 11. 6 (Identity Management) hold their 3 Intemational Summer School on "The Future of Identity in the Infonnation Society" in cooperation with the EU Network of Excellence FIDIS at Karlstad University. The Summer School addressed the theme of Identity Management in relation to current and future technologies in a variety of contexts. The aim of the IFIP summer schools has been to introduce participants to the social implications of Infonnation Technology through the process of infonned discussion. Following the holistic approach advocated by the involved IFIP working groups, a diverse group of participants ranging from young doctoral students to leading researchers in the field were encouraged to engage in discussion, dialogue and debate in an infonnal and supportive setting. The interdisciplinary, and intemational, emphasis of the Summer School allowed for a broader understanding of the issues in the technical and social spheres.

Data Protection and Privacy - Ronald Leenes 2018-12-13 The subjects of Privacy and Data Protection are more relevant than ever, and especially since 25 May 2018, when the European General Data Protection Regulation became enforceable. This volume brings together papers

that offer conceptual analyses, highlight issues, propose solutions, and discuss practices regarding privacy and data protection. It is one of the results of the eleventh annual International Conference on Computers, Privacy, and Data Protection, CPDP 2018, held in Brussels in January 2018. The book explores the following topics: biometrics and data protection in criminal justice processing, privacy, discrimination and platforms for men who have sex with men, mitigation through data protection instruments of unfair inequalities as a result of machine learning, privacy and human-robot interaction in robotized healthcare, privacy-by-design, personal data protection of deceased data subjects, large-scale face databases and the GDPR, the new Europol regulation, rethinking trust in the Internet of Things, fines under the GDPR, data analytics and the GDPR, and the essence of the right to the protection of personal data. This interdisciplinary book was written while the reality of the General Data Protection Regulation 2016/679 was becoming clear. It discusses open issues and daring and prospective approaches. It will serve as an insightful resource for readers with an interest in computers, privacy and data protection.

Security and Privacy in Biometrics - Patrizio Campisi 2013-06-28

This important text/reference presents the latest secure and privacy-compliant techniques in automatic human recognition. Featuring viewpoints from an international selection of experts in the field, the comprehensive coverage spans both theory and practical implementations, taking into consideration all ethical and legal issues. Topics and features: presents a unique focus on novel approaches and new architectures for unimodal and multimodal template protection; examines signal processing techniques in the encrypted domain, security and privacy leakage assessment,

and aspects of standardization; describes real-world applications, from face and fingerprint-based user recognition, to biometrics-based electronic documents, and biometric systems employing smart cards; reviews the ethical implications of the ubiquity of biometrics in everyday life, and its impact on human dignity; provides guidance on best practices for the processing of biometric data within a legal framework.

Biometrics: Concepts, Methodologies, Tools, and Applications - Management Association, Information Resources 2016-08-30

Security and authentication issues are surging to the forefront of the research realm in global society. As technology continues to evolve, individuals are finding it easier to infiltrate various forums and facilities where they can illegally obtain information and access. By implementing biometric authentications to these forums, users are able to prevent attacks on their privacy and security. Biometrics: Concepts, Methodologies, Tools, and Applications is a multi-volume publication highlighting critical topics related to access control, user identification, and surveillance technologies. Featuring emergent research on the issues and challenges in security and privacy, various forms of user authentication, biometric applications to image processing and computer vision, and security applications within the field, this publication is an ideal reference source for researchers, engineers, technology developers, students, and security specialists.

Privacy and Data Protection Issues of Biometric Applications - Els J. Kindt 2013-12-05

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.

Bio-Privacy - Nancy Yue Liu 2013-03

Bio-Privacy: Privacy Regulations and the Challenge of Biometrics provides an in-depth consideration of the legal issues posed by the use of biometric technology. Focusing particularly on the relationship between the use of this

technology and the protection of privacy, this book draws on material across a range of jurisdictions in order to explore several key questions. What are the privacy issues in the biometric context? How are these issues currently dealt with under the law? What principles are applied? Is the current regulation satisfactory? Is it applied consistently? And, more generally, what is the most appropriate way to deal with the legal implications of biometrics? Offering an analysis, and recommendations, with a view to securing adequate human rights and personal data protection, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics will be an important reference point for those with interests in the tension between freedom and security.

The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security - United States. Congress. Senate. Committee on the Judiciary 2008

Selfie Biometrics - Ajita Rattani 2019-09-21

This book highlights the field of selfie biometrics, providing a clear overview and presenting recent advances and challenges. It also discusses numerous selfie authentication techniques on mobile devices. Biometric authentication using mobile devices is becoming a convenient and important means of verifying identity for secured access and services such as telebanking and electronic transactions. In this context, face and ocular biometrics in the visible spectrum has gained increased attention from the research community. However, device mobility and operation in uncontrolled environments mean that facial and ocular images captured with mobile devices exhibit substantial degradation as a result of adverse lighting conditions, specular reflections and motion and defocus blur. In addition, low spatial resolution and the small sensor of front-facing mobile cameras further degrade the sample quality,

reducing the recognition accuracy of face and ocular recognition technology when integrated into smartphones. Presenting the state of the art in mobile biometric research and technology, and offering an overview of the potential problems in real-time integration of biometrics in mobile devices, this book is a valuable resource for final-year undergraduate students, postgraduate students, engineers, researchers and academics in various fields of computer engineering.

Multimodal Biometric Systems - Rashmi Gupta 2021-09-26

Many governments around the world are calling for the use of biometric systems to provide crucial societal functions, consequently making it an urgent area for action. The current performance of some biometric systems in terms of their error rates, robustness, and system security may prove to be inadequate for large-scale applications to process millions of users at a high rate of throughput. This book focuses on fusion in biometric systems. It discusses the present level, the limitations, and proposed methods to improve performance. It describes the fundamental concepts, current research, and security-related issues. The book will present a computational perspective, identify challenges, and cover new problem-solving strategies, offering solved problems and case studies to help with reader comprehension and deep understanding. This book is written for researchers, practitioners, both undergraduate and post-graduate students, and those working in various engineering fields such as Systems Engineering, Computer Science, Information Technology, Electronics, and Communications.

Protecting the Genetic Self from Biometric Threats: Autonomy, Identity, and Genetic Privacy - Akrivopoulou, Christina M. 2015-02-28

Privacy is a fundamental concern of all individuals in the modern information-driven society, but information

security goes beyond digital and data-oriented approaches to include the basic components of what makes us human. Protecting the Genetic Self from Biometric Threats: Autonomy, Identity, and Genetic Privacy considers all aspects of privacy and security relating to an individual's DNA. With a concentration on fundamental human rights as well as specific cases and examples, this essential reference brings pertinent, real-world information to researchers, scientists, and advocates for greater security and privacy in the modern world.

Biometric Recognition - National Research Council 2010-12-12

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.

Biometric Identification, Law and Ethics - Marcus Smith 2021-12-10

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.

Biometric Security and Privacy - Richard Jiang 2016-12-21

This book highlights recent research advances on biometrics using new methods such as deep learning, nonlinear graph embedding, fuzzy approaches, and ensemble learning. Included are special biometric technologies related to privacy and security issues, such as cancellable biometrics and soft biometrics. The book also focuses on several emerging topics such as big data issues, internet of things, medical biometrics, healthcare, and robot-human interactions. The authors show how these new applications have triggered a number of new biometric

approaches. They show, as an example, how fuzzy extractor has become a useful tool for key generation in biometric banking, and vein/heart rates from medical records can also be used to identify patients. The contributors cover the topics, their methods, and their applications in depth.

Cyber Privacy - April Falcon Doss 2020-10-20

"Chilling, eye-opening, and timely, Cyber Privacy makes a strong case for the urgent need to reform the laws and policies that protect our personal data. If your reaction to that statement is to shrug your shoulders, think again. As April Falcon Doss expertly explains, data tracking is a real problem that affects every single one of us on a daily basis." —General Michael V. Hayden, USAF, Ret., former Director of CIA and NSA and former Principal Deputy Director of National Intelligence You're being tracked. Amazon, Google, Facebook, governments. No matter who we are or where we go, someone is collecting our data: to profile us, target us, assess us; to predict our behavior and analyze our attitudes; to influence the things we do and buy—even to impact our vote. If this makes you uneasy, it should. We live in an era of unprecedented data aggregation, and it's never been more difficult to navigate the trade-offs between individual privacy, personal convenience, national security, and corporate profits. Technology is evolving quickly, while laws and policies are changing slowly. You shouldn't have to be a privacy expert to understand what happens to your data. April Falcon Doss, a privacy expert and former NSA and Senate lawyer, has seen this imbalance in action. She wants to empower individuals and see policy catch up. In Cyber Privacy, Doss demystifies the digital footprints we leave in our daily lives and reveals how our data is being used—sometimes against us—by the private sector, the government, and even our employers and schools. She explains the trends in data science,

technology, and the law that impact our everyday privacy. She tackles big questions: how data aggregation undermines personal autonomy, how to measure what privacy is worth, and how society can benefit from big data while managing its risks and being clear-eyed about its cost. It's high time to rethink notions of privacy and what, if anything, limits the power of those who are constantly watching, listening, and learning about us. This book is for readers who want answers to three questions: Who has your data? Why should you care? And most important, what can you do about it?

Biometric System and Data Analysis - Ted Dunstone 2008-10-31

This book brings together aspects of statistics and machine learning to provide a comprehensive guide to evaluating, interpreting and understanding biometric data. It naturally leads to topics including data mining and prediction to be examined in detail. The book places an emphasis on the various performance measures available for biometric systems, what they mean, and when they should and should not be applied. The evaluation techniques are presented rigorously, however they are always accompanied by intuitive explanations. This is important for the increased acceptance of biometrics among non-technical decision makers, and ultimately the general public.

Privacy and Data Protection Issues of Biometric Applications - Els J. Kindt 2016-08-23

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.

Research Anthology on Privatizing and Securing Data - Management Association, Information Resources 2021-04-23

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to

take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.

EU Criminal Law - Valsamis Mitsilegas 2022-05-05

This is the second edition of EU Criminal Law, which has become since its publication in 2009 a key point of reference in the field. The second edition is updated and substantially expanded, to take into account the significant growth of EU criminal law as a distinct legal field and the impact of the entry into force of the Lisbon Treaty on European integration in criminal matters. The book offers a holistic and in-depth analysis of the key elements of European integration in criminal matters, including EU powers and competence to

criminalise, the evolution of judicial co-operation under the principles of mutual recognition and mutual trust, EU action in the field of criminal procedure including legislation on the rights of the defendant and the victim, the evolving role of European bodies and agencies (such as Europol, Eurojust and the European Public Prosecutor's Office) in European criminal law, and the development of EU-wide surveillance and data gathering and exchange mechanisms. Several chapters are devoted to the external dimension of EU action in criminal matters (including transatlantic counter-terrorism cooperation and the impact of Brexit on EU Criminal Law) Throughout the volume, the constitutional and fundamental rights implications of European integration in criminal matters are highlighted. Covering all the key principles of EU law, with clear explanation and rigorous analysis, this will give scholars, students, policy makers and legal practitioners interested in the subject a strong understanding of this fascinating but sometimes complex field.

Biometric Data and New Technologies - The Law and Practical Issues on Technologies Such as CCTV, Facial Recognition and Drones - Melissa Stock 2022-03-18

This book is for legal practitioners, privacy professionals, data protection officers, and any organisation that is using or developing modern technologies that process biometric data. How the law deals with biometrics, CCTV, facial recognition and other technologies is explored and each chapter includes any current and relevant case law. The book also covers best practice for organisations to follow, the recommendations of regulators and future trends. ABOUT THE AUTHOR Melissa Stock is a barrister practising in data, privacy and information law. She advises and represents individuals, companies, and non-governmental organisations in all areas of privacy and data protection. Melissa also advises

on data governance issues and the use of data more broadly in a policy and international context. She writes a blog and produces podcasts. CONTENTS Chapter One - Introduction Chapter Two - Privacy and Data Protection Chapter Three - The General Data Protection Regulations and the Data Protection Act 2018 Chapter Four - Biometric Data Chapter Five - CCTV Chapter Six - Drones Chapter Seven - Facial Recognition Chapter Eight - Emotion Recognition Chapter Nine - Artificial Intelligence Chapter Ten - Conclusion

Biometric Security - Jiankun Hu 2015-02-05

Modern biometrics delivers an enhanced level of security by means of a “proof of property”. The design and deployment of a biometric system, however, hide many pitfalls, which, when underestimated, can lead to major security weaknesses and privacy threats. Issues of concern include biometric identity theft and privacy invasion because of the strong connection between a user and his identity. This book showcases a collection of comprehensive references on the advances of biometric security technology. It compiles a total of fourteen articles, all contributed by thirty-two eminent researchers in the field, thus providing concise and accessible coverage of not only general issues, but also state-of-the-art solutions. The book is divided into five parts: (1) Biometric Template Protection, which covers cancellable biometrics and parameter management protocol; (2) Biometric Key and Encryption, focusing on biometric key generation and visual biometric cryptography; (3) Biometric Systems Analysis, dealing with biometric system security, and privacy evaluation and assessment; (4) Privacy-Enhanced Biometric Systems, covering privacy-enhanced biometric system protocol design and implementation; and (5) Other Biometric Security Technologies. The book will be of particular interest to researchers, scholars, graduate students, engineers,

practitioners and developers interested in security and privacy-related issues in biometric systems. It will also be attractive to managers of various organizations with strong security needs.

Second Generation Biometrics: The Ethical, Legal and Social Context - Emilio Mordini 2012-05-02

While a sharp debate is emerging about whether conventional biometric technology offers society any significant advantages over other forms of identification, and whether it constitutes a threat to privacy, technology is rapidly progressing. Politicians and the public are still discussing fingerprinting and iris scan, while scientists and engineers are already testing futuristic solutions. Second generation biometrics - which include multimodal biometrics, behavioural biometrics, dynamic face recognition, EEG and ECG biometrics, remote iris recognition, and other, still more astonishing, applications – is a reality which promises to overturn any current ethical standard about human identification. Robots which recognise their masters, CCTV which detects intentions, voice responders which analyse emotions: these are only a few applications in progress to be developed. This book is the first ever published on ethical, social and privacy implications of second generation biometrics. Authors include both distinguished scientists in the biometric field and prominent ethical, privacy and social scholars. This makes this book an invaluable tool for policy makers, technologists, social scientists, privacy authorities involved in biometric policy setting. Moreover it is a precious instrument to update scholars from different disciplines who are interested in biometrics and its wider social, ethical and political implications.

Privacy and Data Protection Challenges in the Distributed Era - Eugenia Politou 2021-10-22

This book examines the conflicts arising from the implementation of privacy

principles enshrined in the GDPR, and most particularly of the ``Right to be Forgotten'', on a wide range of contemporary organizational processes, business practices, and emerging computing platforms and decentralized technologies. Among others, we study two ground-breaking innovations of our distributed era: the ubiquitous mobile computing and the decentralized p2p networks such as the blockchain and the IPFS, and we explore their risks to privacy in relation to the principles stipulated by the GDPR. In that context, we identify major inconsistencies between these state-of-the-art technologies with the GDPR and we propose efficient solutions to mitigate their conflicts while safeguarding the privacy and data protection rights. Last but not least, we analyse the security and privacy challenges arising from the COVID-19 pandemic during which digital technologies are extensively utilized to surveil people’s lives.