Read Online Current And Future Uses Of Biometric Data And Technologies Government Response To The Committee Sixth Report Of Session 2014 15 Second Special Report Of Session 2015 16 House Of Commons Papers

Thank you enormously much for downloading **Current And Future Uses Of Biometric Data And Technologies Government Response To The Committee Sixth Report Of Session 2014 15 Second Special Report Of Session 2015 16 House Of Commons Papers**.Maybe you have knowledge that, people have see numerous time for their favorite books subsequent to this Current And Future Uses Of Biometric Data And Technologies Government Response To The Committee Sixth Report Of Session 2014 15 Second Special Report Of Session 2015 16 House Of Commons Papers, but end up in harmful downloads.

Rather than enjoying a good ebook next a mug of coffee in the afternoon, on the other hand they juggled next some harmful virus inside their computer. **Current And Future Uses Of Biometric Data And Technologies Government Response To The Committee Sixth Report Of Session 2014 15 Second Special Report Of Session 2015 16 House Of Commons Papers** is understandable in our digital library an online access to it is set as public for that reason you can download it instantly. Our digital library saves in fused countries, allowing you to acquire the most less latency times to download any of our books similar to this one. Merely said, the Current And Future Uses Of Biometric Data And Technologies Government Response To The Committee Sixth Report Of Session 2014 15 Second Special Report Of Session 2015 16 House Of Commons Papers is universally compatible bearing in mind any devices to read.

KEY=16 - HOOPER QUINN

HC 734 - CURRENT AND FUTURE USES OF BIOMETRIC DATA AND TECHNOLOGIES

The Stationery Office

CURRENT AND FUTURE USES OF BIOMETRIC DATA AND TECHNOLOGIES

GOVERNMENT RESPONSE TO THE COMMITTEE' SIXTH REPORT OF SESSION 2014-15, SECOND SPECIAL REPORT OF SESSION 2015-16

Government response to HC 734, session 2014-15 (ISBN 9780215083845)

PRIVACY AND DATA PROTECTION ISSUES OF BIOMETRIC APPLICATIONS

A COMPARATIVE LEGAL ANALYSIS

Springer Science & Business Media 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.

THE CURRENT AND FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGIES

JOINT HEARING BEFORE THE SUBCOMMITTEE ON RESEARCH & SUBCOMMITTEE ON TECHNOLOGY, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY, HOUSE OF REPRESENTATIVES, ONE HUNDRED THIRTEENTH CONGRESS, FIRST SESSION, TUESDAY, MAY 21, 2013

BIOMETRIC RECOGNITION

CHALLENGES AND OPPORTUNITIES

National Academies Press 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.

SUMMARY OF A WORKSHOP ON THE TECHNOLOGY, POLICY, AND CULTURAL DIMENSIONS OF BIOMETRIC SYSTEMS

National Academies Press 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.

BIOMETRICS

John Wiley & Sons Market_Desc: · CIOs· CTOs· IT Managers· Security Directors· Technical staff who work with biometrics on a daily basis (network administrators, programmers)· Sales, marketing, and customer service staff at companies that sell biometric products Special Features: · First book to give the lay person an overview of available biometric technologies and discuss key issues for a successful deployment· Reviews various biometric technologies such as finger-scan, iris-scan, facial-scan, voice-scan, signature-scan, hand-scan, and others· Explores privacy concerns, areas of current industry use, and offers large-scale project examples About The Book: This is the first book to give the lay person an overview of available biometric technologies, and discuss key issues for a successful deployment. This textbook covers Biometric technologies: Finger-scan, iris-scan, facial-scan, voice-scan, signature-scan, hand-scan, and other biometrics; Areas of industry use, current and future; Building a business case for biometrics and Privacy concerns.

A QUESTION OF TRUST

Lulu.com

BIOMETRIC IDENTIFICATION, LAW AND ETHICS

Springer Nature 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.

BIOMETRY

TECHNOLOGY, TRENDS AND APPLICATIONS

CRC Press Biometrics provide quantitative representations of human features, physiological and behavioral. This book is a compilation of biometric technologies developed by various research groups in Tecnologico de Monterrey, Mexico. It provides a summary of biometric systems as a whole, explaining the principles behind physiological and behavioral biometrics and exploring different types of commercial and experimental technologies and current and future applications in the fields of security, military, criminology, healthcare education, business, and marketing. Examples of biometric systems using brain signals or electroencephalography (EEG) are given. Mobile and home EEG use in children's natural environments is covered. At the same time, some examples focus on the relevance of such technology in monitoring epileptic encephalopathies in children. Using reliable physiological signal acquisition techniques, functional Human Machine Interfaces (HMI) and Brain-Computer Interfaces (BCI) become possible. This is the case of an HMI used for assistive navigation systems, controlled via voice commands, head, and eye movements. A detailed description of the BCI framework is presented, and applications of user-centered BCIs, oriented towards rehabilitation, human performance, and treatment monitoring are explored. Massive data acquisition also plays an essential role in the evolution of biometric systems. Machine learning, deep learning, and Artificial Intelligence (AI) are crucial allies here. They allow the construction of models that can aid in early diagnosis, seizure detection, and data-centered medical decisions. Such techniques will eventually lead to a more concise understanding of humans.

BIOMETRIC-BASED PHYSICAL AND CYBERSECURITY SYSTEMS

Springer 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.

HC 758 - LEGACY-PARLIAMENT 2010-15

The Stationery Office

CURRENT SECURITY MANAGEMENT & ETHICAL ISSUES OF INFORMATION TECHNOLOGY

IGI Global "This scholarly examination of the ethical issues in information technology management covers basic details such as improving user education and developing security requirements as well as more complicated and far-reaching problems such as protecting infrastructure against information warfare. Social responsibility is analyzed with global examples and applications, including knowledge-based society in Latin America, socioeconomics factors of technology in the United States, and system ethics in the Arab world."

THE BIOMETRIC INDUSTRY REPORT - FORECASTS AND ANALYSIS TO 2006

Elsevier Biometrics - the physiological and/or behavioural characteristics that can be used to verify the identity of an individual - are no longer just being used in high security locations; they are now in use in major, mainstream government and commercial applications. Since September 11, the heightened awareness of security issues is driving forward the adoption of biometrics within numerous application environments. Coupled with a dramatic decrease in the price of such systems and the formulation of comprehensive industry standards, the market looks set for rapid growth over the next 5 years. The second edition of The Biometric Industry Report - Forecasts and Analysis to 2006 examines the current use and future growth of biometrics. It analyses the trends in markets, technologies and industry structure and profiles the major players. The report provides key market statistics and forecasts essential for companies to plot their future growth strategies. For a PDF version of the report please call Sarah Proom on +44 (0) 1865 843181 for price details.

GUIDE TO BIOMETRICS FOR LARGE-SCALE SYSTEMS

TECHNOLOGICAL, OPERATIONAL, AND USER-RELATED FACTORS

Springer Science & Business Media 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.

THE PRACTITIONER'S GUIDE TO BIOMETRICS

American Bar Association 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.

HC 573 - INVESTIGATORY POWERS BILL: TECHNOLOGY ISSUES

The Stationery Office The draft Investigatory Powers Bill was published by the Government on 4 November 2015. Ministers have been clear that the intention of this Bill is to consolidate and clarify existing legislation on the interception of communications and the acquisition of communications data and to modernise the law in the light of developments in communications technologies, in order to maintain the operational capabilities of law enforcement agencies and the intelligence and security services. Previous attempts to legislate in this area have met with criticisms over the lack of consultation with communications service providers (CSPs) on matters of technical feasibility and cost. In our inquiry we have focused on technological aspects of the draft Bill in order to identify the main technological issues involved and how these might affect the communications businesses that will have to collect data and cooperate with the security authorities. If law enforcement agencies and the intelligence and security services are effectively to combat terrorism and serious crime, they must have the means to keep pace with developments in communications. They will doubtless need to continue to deploy a range of methods for intercepting and acquiring information about communications. The evidence we have received suggests there are still many unanswered questions about how this legislation will work in the fast moving world of technological innovation. It is essential that the integrity and security of legitimate online transactions is maintained if we are to trust in, and benefit from, the opportunities of an increasingly digital economy.

HC 469 - SCIENCE IN EMERGENCIES: UK LESSONS FROM EBOLA

The Stationery Office Ebola is a rare and deadly disease. Since late 2013, West Africa has experienced the largest Ebola outbreak ever recorded. We pay tribute to all those who worked tirelessly to tackle this outbreak, some of whom gave evidence to this inquiry, and many of whom continue working to avert similar crises in the future. We also commend the Government on its leading contribution to the fight against Ebola, and the financial, and personnel, commitments that it made, from constructing and staffing Ebola treatment centres in Sierra Leone to deploying troops, helicopters, aircrew and an aviation support ship to provide much needed logistical support. Examples of UK successes in tackling Ebola, however, must not allow complacency to set in. Despite this impressive deployment of resources to combat Ebola in Sierra Leone, the UK response - like the international response - was undermined by systemic delay. The biggest lesson that must be learnt from this outbreak of Ebola is that

even minor delays in responding cost lives. Yet delays were evident at every stage of our response, from escalating Public Health England's disease surveillance data to those with the capacity to act, to convening a Scientific Advisory Group for Emergencies which failed to be established until October 2014, three months after 'Cobra', the Government's emergency response committee, first met. In the absence of established mechanisms, ad hoc approaches emerged to fill the gaps. Inevitably, these were not as effective, or as targeted, as they should have been.

RECENT ADVANCES IN BIOMETRICS

BoD – Books on Demand Biometrics are widely used in various real-life applications, including personal recognition, identification, verification, and more. They may also be used for safety, security, permission, banking, crime prevention, forensics, medical applications, and communication. This book explores the latest developments, theories, methods, approaches, algorithms, analysis, systems, hardware, and software in biometrics and related systems.

BIOMETRY

TECHNOLOGY, TRENDS AND APPLICATIONS

CRC Press Biometric systems allow a quantitative approach to the representation of humans. Different techniques enable the use of physiological and behavioral information from human processes. These data can be obtained and studied for various purposes.

VIOLENT EXTREMISM: BREAKTHROUGHS IN RESEARCH AND PRACTICE

BREAKTHROUGHS IN RESEARCH AND PRACTICE

IGI Global Advances in digital and other technologies have provided ample positive impacts to modern society; however, in addition to such benefits, these innovations have inadvertently created a new venue for terrorist activities. Examining violent extremism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Violent Extremism: Breakthroughs in Research and Practice is a critical source of academic knowledge on the social, psychological, and political aspects of radicalization and terrorist recruitment. Highlighting a range of pertinent topics such as counterterrorism, propaganda, and online activism, this publication is an ideal reference source for researchers, analysts, intelligence officers, policymakers, academicians, researchers, and graduate-level students interested in current research on violent extremism.

BIOMETRICS, CRIME AND SECURITY

Routledge This book addresses the use of biometrics – including fingerprint identification, DNA identification and facial recognition – in the criminal justice system: balancing the need to ensure society is protected from harms, such as crime and terrorism, while also preserving individual rights. It offers a comprehensive discussion of biometric identification that includes a consideration of: basic scientific principles, their historical development, the perspectives of political philosophy, critical security and surveillance studies; but especially the relevant law, policy and regulatory issues. Developments in key jurisdictions where the technology has been implemented, including the United Kingdom, United States, Europe and Australia, are examined. This includes case studies relating to the implementation of new technology, policy, legislation, court judgements, and where available, empirical evaluations of the use of biometrics in criminal justice systems. Examples from non-western areas of the world are also considered. Accessibly written, this book will be of interest to undergraduate, postgraduate and research students, academic researchers, as well as professionals in government, security, legal and private sectors.

BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS

Elsevier 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/authentication 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

HANDBOOK OF BIOMETRICS

Springer Science & Business Media Biometrics is a rapidly evolving field with applications ranging from accessing one's computer to gaining entry into a country. The deployment of large-scale biometric systems in both commercial and government applications has increased public awareness of this technology. Recent years have seen significant growth in biometric research resulting in the development of innovative sensors, new algorithms, enhanced test methodologies and novel applications. This book addresses this void by inviting some of the prominent researchers in Biometrics to contribute chapters describing the fundamentals as well as the latest innovations in their respective areas of expertise.

INNOVATIONS IN COMPUTING SCIENCES AND SOFTWARE ENGINEERING

Springer Science & Business Media Innovations in Computing Sciences and Software Engineering includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Computer Science, Software Engineering, Computer Engineering, and Systems Engineering and Sciences. Topics Covered: •Image and Pattern Recognition: Compression, Image processing, Signal Processing Architectures, Signal Processing for Communication, Signal Processing Implementation, Speech Compression, and Video Coding Architectures. •Languages and Systems: Algorithms, Databases, Embedded Systems and Applications, File Systems and I/O, Geographical Information Systems, Kernel and OS Structures, Knowledge Based Systems, Modeling and Simulation, Object Based Software Engineering, Programming Languages, and Programming Models and tools. •Parallel Processing: Distributed Scheduling, Multiprocessing, Real-time Systems, Simulation Modeling and Development, and Web Applications. •Signal and Image Processing: Content Based Video Retrieval, Character Recognition, Incremental Learning for Speech Recognition, Signal Processing Theory and Methods, and Vision-based Monitoring Systems. •Software and Systems: Activity-Based Software Estimation, Algorithms, Genetic Algorithms, Information Systems Security, Programming Languages, Software Protection Techniques, Software Protection Techniques, and User Interfaces. •Distributed Processing: Asynchronous Message Passing System, Heterogeneous Software Environments, Mobile Ad Hoc Networks, Resource Allocation, and Sensor Networks. •New trends in computing: Computers for People of Special Needs, Fuzzy Inference, Human Computer Interaction, Incremental Learning, Internet-based Computing Models, Machine Intelligence, Natural Language.

SECOND GENERATION BIOMETRICS: THE ETHICAL, LEGAL AND SOCIAL CONTEXT

Springer Science & Business Media 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.

VALUES ISSUES IN BIOMETRIC DATA COLLECTION

Since the events of 9/11, the United States has placed biometrics at the heart of its national security policy beginning by collecting fingerprints as well as iris and facial scans from visitors before they enter into the U.S. Collection of these biometrics ensures that the government identifies criminals before they enter into the U.S. or obtain a visa. Biometric collection also assists in identifying those who commit a crime while residing legally in the U.S. The problem with this strategy is that biometric information is extremely sensitive, as it is unique to only you. As a result, there are a number of privacy and social concerns surrounding biometric collection, particularly as biometrics are now required to travel virtually anywhere in the world. Additionally, as biometrics are a relatively new technology, technological problems exist which can lead to negative public perceptions. In order to examine the issues associated with collection of biometric data, legislation mandating biometrics was reviewed, personal interviews with government employees connected to biometric programs were conducted, privacy, social and foreign concerns in collecting biometric data was researched, indirect negative consequences of biometrics (profiling, surveillance, data breeches) was looked at and future uses of this technology based on current functionality was determined. All of the information collected resulted in a common

conclusion - biometrics will continue to shape the future for identity management and national security by reducing identity theft and terrorist acts. Sharing U.S. collected biometric data with other allied democratic nations will improve global national security. While privacy issues will continue to surface regarding biometric data, the U.S. government will continue to ensure that our privacy is protected through privacy assessment impact analyses of future biometric collection programs. Commercial and governmental organizations will continue to find new uses for biometrics that will make life easier for individuals globally. These new innovations will also result in rapid profitability for biometric industries in the upcoming years.

BIOMETRICS IN THE NEW WORLD

THE CLOUD, MOBILE TECHNOLOGY AND PERVASIVE IDENTITY

Springer Science & Business Media This book takes a fresh look at biometrics and identity management, extending the dialogue beyond technical considerations, and exploring some of the broader societal and philosophical aspects surrounding the use of biometric applications. Features: presents a brief history of the development of biometrics, and describes some of the popularly held misconceptions surrounding the technology; investigates the challenges and possibilities of biometrics across third party infrastructures and on mobile computing devices; provides guidance on biometric systems design; explores the mechanisms necessary to enable identity intelligence, including logging mechanisms, data communications and data formats; discusses such usage issues as collaboration frameworks, and messaging and data translation; examines the impact of biometric technologies on society, covering issues of privacy and user factors; reviews the current situation in identity management, and predicts where these trends may take us in the future.

SMART INNOVATIONS IN ENGINEERING AND TECHNOLOGY

Springer Nature This easy-to-understand book discusses applications of current technologies and the foundations for their extension into emerging areas in the future. It includes research presented at two conferences: 5th International IBM Cloud Academy Conference, 2017, held in Wrocław, Poland. 5th Asia-Pacific Conference on Computer Assisted and System Engineering, 2017, held in Guilin, China. These conferences focused on system and application engineering, including achievements in the interdisciplinary topics of cloud computing, big data, IoT and mobile communications. Featuring 19 chapters, the book has the potential to influence current and future research and applications combining the best attributes of computing, mathematics, artificial intelligence, biometrics and software engineering to create a comprehensive research application domain.

BIOMETRICS TECHNOLOGY REVIEW 2008

Biometrics is the measurement of personal physical features, actions or behavioural characteristics that distinguish between individuals. In recent years automated biometric systems, such as facial, fingerprint and iris recognition systems, have been developed to facilitate a range of functions. These functions can be broadly categorised as verification or identification, and include, for instance, physical and logical access control, management of major plant and machinery, weapons control, identity management, surveillance operations, and personnel management. This paper is an updated version of the Biometrics Technology Review 2002 published in 2003 by Blackburn et al. It provides an overview of the basic elements of biometrics; a detailed examination of current and future biometric technologies; discusses the many different applications of biometrics; and highlights the issues associated with using such technology.

BIOMETRIC DATA AND NEW TECHNOLOGIES - THE LAW AND PRACTICAL ISSUES ON TECHNOLOGIES SUCH AS CCTV, FACIAL RECOGNITION AND DRONES

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

ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY

Springer Science & Business Media Expanded into two volumes, the Second Edition of Springer’s Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the

topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition's base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition's editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries, the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text's practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

OUR BIOMETRIC FUTURE

FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE

NYU Press Since the 1960s, a significant effort has been underway to program computers to "see" the human face—to develop automated systems for identifying faces and distinguishing them from one another—commonly known as Facial Recognition Technology. While computer scientists are developing FRT in order to design more intelligent and interactive machines, businesses and states agencies view the technology as uniquely suited for "smart" surveillance—systems that automate the labor of monitoring in order to increase their efficacy and spread their reach. Tracking this technological pursuit, Our Biometric Future identifies FRT as a prime example of the failed technocratic approach to governance, where new technologies are pursued as shortsighted solutions to complex social problems. Culling news stories, press releases, policy statements, PR kits and other materials, Kelly Gates provides evidence that, instead of providing more security for more people, the pursuit of FRT is being driven by the priorities of corporations, law enforcement and state security agencies, all convinced of the technology's necessity and unhindered by its complicated and potentially destructive social consequences. By focusing on the politics of developing and deploying these technologies, Our Biometric Future argues not for the inevitability of a particular technological future, but for its profound contingency and contestability.

THE FUTURE OF IDENTITY IN THE INFORMATION SOCIETY

PROCEEDINGS OF THE THIRD IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS INTERNATIONAL SUMMER SCHOOL ON THE FUTURE OF IDENTITY IN THE INFORMATION SOCIETY, KARLSTAD UNIVERSITY, SWEDEN, AUGUST 4-10, 2007

Springer 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.

BIOMETRIC IDENTIFICATION, LAW AND ETHICS

Springer 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.

FORENSIC SCIENCE

A SOCIOLOGICAL INTRODUCTION

Routledge Forensic Science provides a comprehensive overview of the sociology of forensic science. Drawing on a wealth of international research and case studies, it explores the intersection of science, technology, law and society and examines the production of forensic knowledge. The book explores a range of key topics such as: • The integration of science into police work and criminal investigation • The relationship between law and science • Ethical and social issues raised by new forensic technology including DNA analysis • Media portrayals of forensic science • Forensic policy and the international agenda for forensic science This new edition has been fully updated, particularly with regard to new technology in relation to the various new forms of DNA technology and facial recognition. Updates and additions include: • Facial recognition technology • Digital forensics and its use in policing • Algorithms (such as probabilistic genotyping) • Genealogical searching • Phenotyping This new edition also reviews and critically appraises recent scholarship in the field, and new international case studies have been introduced, providing readers with an international comparative perspective. Engaging with sociological literature to make arguments about the ways in which forensic science is socially constituted and shapes justice, Forensic Science provides an excellent introduction to students about the location of forensic science and the ways it fits within the criminal justice system, as well as systems of professionalisation and ethics. It is important and compelling reading for students taking a range of courses, including criminal investigation, policing, forensic science, and the sociology of science and technology.

PROFILING THE EUROPEAN CITIZEN

CROSS-DISCIPLINARY PERSPECTIVES

Springer Science & Business Media In the eyes of many, one of the most challenging problems of the information society is that we are faced with an ever expanding mass of information. Based on the work done within the European Network of Excellence (NoE) on the Future of Identity in Information Society (FIDIS), a set of authors from different disciplinary backgrounds and jurisdictions share their understanding of profiling as a technology that may be preconditional for the future of our information society.

VEIN PATTERN RECOGNITION

A PRIVACY-ENHANCING BIOMETRIC

CRC Press As one of the most promising biometric technologies, vein pattern recognition (VPR) is quickly taking root around the world and may soon dominate applications where people focus is key. Among the reasons for VPR’s growing acceptance and use: it is more accurate than many other biometric methods, it offers greater resistance to spoofing, it focuses on people and their privacy, and has few negative cultural connotations. Vein Pattern Recognition: A Privacy-Enhancing Biometric provides a comprehensive and practical look at biometrics in general and at vein pattern recognition specifically. It discusses the emergence of this reliable but underutilized technology and evaluates its capabilities and benefits. The author, Chuck Wilson, an industry veteran with more than 25 years of

experience in the biometric and electronic security fields, examines current and emerging VPR technology along with the myriad applications of this dynamic technology. Wilson explains the use of VPR and provides an objective comparison of the different biometric methods in use today—including fingerprint, eye, face, voice recognition, and dynamic signature verification. Highlighting current VPR implementations, including its widespread acceptance and use for identity verification in the Japanese banking industry, the text provides a complete examination of how VPR can be used to protect sensitive information and secure critical facilities. Complete with best-practice techniques, the book supplies invaluable guidance on selecting the right combination of biometric technologies for specific applications and on properly implementing VPR as part of an overall security system.

ENCYCLOPEDIA OF BIOMETRICS

I - Z.

Springer Science & Business Media With an A–Z format, this encyclopedia provides easy access to relevant information on all aspects of biometrics. It features approximately 250 overview entries and 800 definitional entries. Each entry includes a definition, key words, list of synonyms, list of related entries, illustration(s), applications, and a bibliography. Most entries include useful literature references providing the reader with a portal to more detailed information.

LABORATORY MANAGEMENT INFORMATION SYSTEMS: CURRENT REQUIREMENTS AND FUTURE PERSPECTIVES

CURRENT REQUIREMENTS AND FUTURE PERSPECTIVES

IGI Global Technological advances have revolutionized the way we manage information in our daily workflow. The medical field has especially benefitted from these advancements, improving patient treatment, health data storage, and the management of laboratory samples and results. Laboratory Management Information Systems: Current Requirements and Future Perspectives responds to the issue of administering appropriate regulations in a medical laboratory environment in the era of telemedicine, electronic health records, and other e-health services. Exploring concepts such as the implementation of ISO 15189:2012 policies and the effects of e-health application, this book is an integral reference source for researchers, academicians, students of health care programs, health professionals, and laboratory personnel.