



RISE Toolkits for Industry

RISE Public Awareness Campaign

Project funded by the European Commission-FP7
Science and Society Theme
Grant Agreement n : 230389
Coordination Action (CA)
Start date of the project: 1 March 2009
Duration: 36 months



Toolkit for Industry: Factsheets

Rising Pan European and International Awareness of Biometrics and Security Ethics (RISE) is an international initiative for promoting Awareness on Ethical Aspects of Biometrics and Security Technologies. RISE aims to deepen, enlarge, and ensure continuity to European and international dialogue already instigated by the international conferences on ethics and biometrics organised by the EC DG Research and the US DHS Privacy Office respectively in Brussels and Washington DC in 2005 and 2006.

To support the overarching goal of establishing a broad and effective dialogue, the project includes a comprehensive effort to create significant public awareness about the goals and activities of the RISE project. This effort focuses on international and transnational ethical awareness on biometrics and security issues, and is independent and non-partisan. Conferences, meetings, and workshops have been the primary focus of the RISE project, and most of the efforts of the partners are engaged in promoting these venues as the opportunity to share information, perspectives, and to establish and expand dialogue on both an informal and formal basis amongst stakeholders and global actors.

The information in this Toolkit has been compiled from the published RISE reports and workshop presentations given by speakers at the RISE events. Most RISE workshop presentations are posted on the RISE website at www.riseproject.eu. Any additional information in this Toolkit obtained from other sources is appropriately cited throughout.

This Toolkit includes the following factsheets related to the development of biometric technology:

Data, Identity, and Information Security for Biometric Technology	Page 3
Ethical Considerations Related to Developing Biometric Technology.....	Page 6
E-Governance in India	Page 9
E-Governance in China.....	Page 13
Privacy Impact Assessments	Page 15

The RISE project is funded by the European
Commission-FP7 under Grant Agreement n°: 230389.

Data, Identity, and Privacy Security for Biometric Technology



Industry Factsheet 1

KEY FACTS

- The global biometrics industry is estimated by market analysts at between \$3-4 Billion USD in 2009 – to grow to \$11 Billion by 2017.
- The main challenge with biometric technology is how to promote mobility, at the same time minimize the risks to our security and privacy.
- According to a “Chronology of Data Breaches” maintained by Privacy Rights Clearinghouse, over 263 Million records containing sensitive personal information (driver’s license numbers, social security numbers, etc.) have been involved in security breaches in the US since January 2005.
- The US Federal Trade Commission reports that identity theft complaints in calendar year 2008 represented more over 26% of overall complaints received (over 300,000 complaints through various law enforcement sources in the US).
- Cost implications of Data Breach is \$305 per record for a single breach in a high profile regulated organization (Forrester).
- Data Protection has emerged as a major challenge in cross-border data flows. Clients are demanding more security as their worries about the cyber crimes, privacy and identity theft grow.
- Between public and private locations, there are estimated to be more than a half million CCTV cameras in London alone; studies have shown that only one crime is solved per each 1,000 cameras.
- In Europe, biometric data falls under Directive 95/46 regarding personal data protection. Article 25 (6) of the EU Data Protection Directive requires member states to place restrictions on transfers of personal data to third countries that cannot guarantee an adequate level of data protection.

Estimated global mobile populations:

- Refugees /uprooted people 22 million (UNHCR 2002)
- Undocumented Migrants 10 -15 million (ILO 2000)
- International Travelers 698 million (WTO 2000)
- Migrant Workers 70-80 million (ILO 2001)
- Survivors of Trafficking 700,000-2m (U.S. State Dept. 2002)

~ 800 million

Protecting privacy: technology design recommendations

- Revisit design, architecture, and deployment of projects from data security and privacy perspective. Conduct routine privacy impact assessments
- Inculcate data centric approach in the security and privacy initiatives
- Ensure that project implementation and operations adhere to the guidelines and standards for privacy
- Ensure that privacy is ensured in entire lifecycle of data i.e. data collection, use, processing, and storage
- Adopt privacy enhancing technologies, privacy by design principles
- Implement adequate measures for security and vulnerability management of systems that engage in processing of personal information
- Build an organization culture that respect privacy of the end user
- Ensure that privacy policies and practices are defined and implemented
- Ensure that significant effort is dedicated on end user education that enable them to take trust decisions while they are transacting online
- Establish vigilant monitoring for privacy; deploy a mechanism to address end user's grievances

Lowering the risk of privacy invasiveness

- Deploy the system as optional rather than mandatory.
- Use the system for identification rather than verification.
- Deploy the system for a fixed period of time rather than indefinitely.
- Allow the user to interact with the system as an individual/customer rather than as an employee/citizen.
- Allow the system's biometric information to be owned by the enrollee rather than the deploying institution.
- Store the biometric data locally in a personal storage area rather than in a remote database storage facility.
- Deploy biometric technology based on behaviors rather than physiological features.
- Deploy biometric technology that uses biometric templates rather than biometric images.

Need for privacy of security decision makers at European enterprises - Forrester Survey Statistics, Q3-2008, Europe

Top Business Priorities

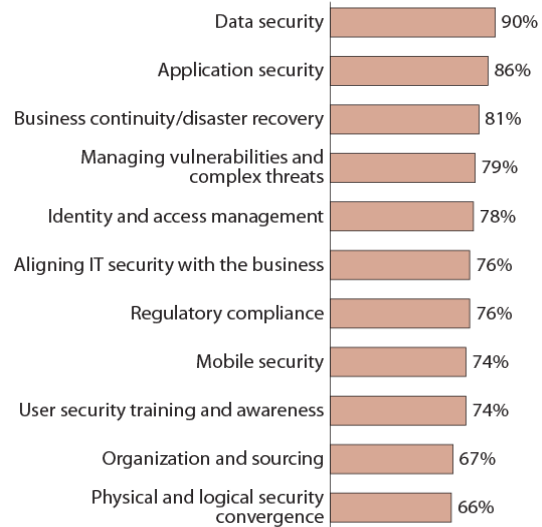
“How important to your IT security group will each of the following business objectives be in the next 12 months?”



Base: 285 decision-makers at European enterprises responding “important” or “very important”

Important Issues

“How important to your IT security organization will each of the following issues be in the next 12 months?”



Base: 285 security decision-makers at European enterprises responding “important” or “very important”

Presentation Sources

- **Emilio Mordini**, Coordinator, Project RISE – Introduction to the Theme of the Conference, September 2009
- **Kush Wadhwa**, Managing Director, Global Security Intelligence – Panel on Differences and Commonalities – Asia, Europe, and the U.S., September 2009
- **Kamlesh Bajaj**, CEO, Data Security Council of India (DSCI) - DSCI and Data Protection, September 2009
- **Xiaomei Zhai**, Center for Bioethics, Chinese Academy of Medical Sciences, Beijing, P. R. China, 'The Status Quo and Ethical Governance in Biometric in Mainland China', January 2010
- **Mr. Vinayak Godse**, Director, Data Security Council of India, Data Security in E-Governance: Projects in India, December 2010
- **Mr. Nicolas Delvaux**, Morpho, PETs for Biometrics, December 2010
- **Ms. Mary Collins**, International Biometric Group, Privacy and Security of Biometric Systems, December 2010

Ethical Considerations Related to Developing Biometric Technology

KEY FACTS

- Biometrics are vulnerable to privacy and security concerns:
 - Biometric matching is based on laws of probability, so one can always expect false matches and false non-matches.
 - Biometrics never give 100% certainty, and can make the wrong associations between individuals' biometric data and their ID documents or data.
 - Biometrics cannot make statements about integrity of ID documents and data that it uses as reference.
 - Biometrics cannot establish identity: it can only recognise individuals with a certain level of accuracy.
- Identification using biometric technology may interfere with privacy rights (art. 8 ECHR; article 7 Union Charter).
- Biometrics is increasingly taking on expanded meanings and contexts.
- Security and privacy considerations stand out as major issues that affect adoption and governance of biometric technology.
- When developing biometric technology, consideration from different angles will lead to different emphases.
- A holistic approach is called for when considering the ethical issues relevant to developing biometric technology.
- Emerging technologies and bundling of established technologies are presenting new ethical challenges:
 - New security technologies are emerging aimed at determination of intent (e.g., US DHS' Future Attribute Screening Technologies) using multi-modal behavioral and physiological sensing technologies
 - Most mobile phones are now equipped with GPS/GSM for emergency-based locating – presenting implications for surveillance

Benefits and Risks of Biometrics

Benefits

- Security (monitor migration, combat identity theft and fraud)
- Economic (cut costs produce efficiency gains for administration)
- Convenience in time (avoid queues, faster answers, immediate access to information)
- Mobility (vote anywhere, services and movement of capital across borders via e-services)

Risks

- Threat to privacy (increasing tension between the principle of security and that of privacy and democracy)
- Potential of social exclusion (border surveillance has divergent effects for different groups of people)
- Securitisation (more and more issues framed in terms of security concerns)
- Changing social relationships (climate of suspicion)

Rapidly changing scope for ethics, policies and regulations

- The global ICT infrastructure is rapidly changing with major implications on user behaviours
- The notion of biometrics “belonging” to individually identified persons is changing with ICT advancements
- The scope for policies, regulations and ethics is fast changing as a result
- New applications of technology may lead to frequent and voluntary use of biometric data
- The scope for ethical and policy considerations becomes even more multifarious and complex

Presentation Sources

- **Emilio Mordini**, Coordinator, Project RISE, Identity in the post Weakileaks era, 44th Meeting of the European Group on Ethics in Science and new technologies (EGE) – Brussels 13 April 2011
- **Emilio Mordini**, Biometric Technologies: the societal and political context, 8th Summer School for advanced studies on biometrics for secure authentication, Alghero 10th June 2011
- **Kush Wadhwa**, Managing Director, Global Security Intelligence – Panel on Differences and Commonalities – Asia, Europe, and the U.S., September 2009
- **Margit Sutrop**, University of Tartu, Estonia, Global Mobility and Security: Ethics and policy of biometrics, March 2010
- **Mr. Ronald Huijgens**, Director Biometric Technologies, Unisys, The challenge of building safe and reliable biometric systems, December 2010

E-Governance in India



Industry Factsheet 3

E-governance agenda and objectives for India

- India's Unique ID programme implementation to collect biometrics from more than 10% of the world's population over the next several years
- *Wireless Broadband and Mobile Access* in all towns and villages
- Common Service Centres (CSCs) in all villages
- All major public services available online
- All major public services available through call centres
- Individual ID scheme fully operational
- Integrate Financial Services and Mobile telephony
- Integrate ID services with mobile telephony
- Create complete range of high quality educational programmes for school and college level available online and integrated into the regular curriculum
- Major agriculture sector services including consultancy, credit and insurance available online
- High quality medical services available in villages through telemedicine
- Provision of Insurance services (crop, health, life, etc.)
- Create an open technology generic integrated platform for e-governance that can be used by governments worldwide backed by strong support services by Indian IT industry and manpower
- Position India as a hub for a number of ICT-related technologies relevant for developing/ multi-lingual countries
- Draw up and implement a national programme to position India as a global centre for IT security services which also support a secure cyber space in the country

	<ul style="list-style-type: none"> • Adopt an <i>E-Governance Law</i> • Exchange of information with citizens, businesses or other government departments • Speedier and more efficient delivery of public services • Improve internal efficiency • Reduce costs or increasing revenue • Re-structure of administrative processes • Ensure participation of the people • Transparency, limited leakage, targeted social benefits, etc.
<p>India e-governance considerations affecting data security and privacy</p>	<ul style="list-style-type: none"> • Society recognized as having a diverse culture and perceptions. • Society where illiteracy is a significant challenge. • Society where communal politics still prevails. • Society where practice of renting creates huge problem in public services delivery. • Country which is situated in one of the most challenging geopolitical area leading to strong focus on national security against privacy.
<p>India data protection challenges</p>	<ul style="list-style-type: none"> • Large centralized databases, accessible over networks in real-time, presents significant operational and security concerns. If networks fail or become unavailable, the entire identification system collapses • Large centralized databases of biometric PII, hooked up to networks and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities to exploit. • Large centralized databases are more prone to functional creep (secondary uses) and insider abuse. • Significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection.

National projects in India making use of biometrics

Private organizations are using biometrics for controlling Data Center Access, Critical System Access, and ecommerce transactions. E-Governance, with a budget of over \$ 6 billion, is rolling out 26 projects. Some of these projects that use biometrics are the following:

- Biometric Passports in India by 2010
- Biometric PAN card using iris scan
- Planning use of Biometric card for beneficiaries of NREG, SSP
- Integrated Prisons Management Systems
- Health Management Information Systems [HMIS]

Various agencies including DSCI are engaged in promoting biometrics ethics:

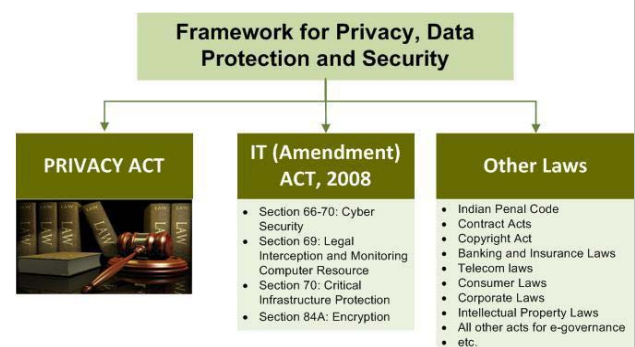
- Incorporate biometric data as a personal information – rules for IT Act (Amendment) 2008
- Ethics standards for biometric use by NISG (National Institute of Smart Governance)
- Awareness campaign for users, vendors, organizations and policy makers

Important Indian data protection legislation and compliance measures

- The Indian legal system deals with cyber security and data protection measures in various enactments, namely:

- The Indian Telegraph Act, 1885
- The Indian Contract Act, 1872
- The Specific Relief Act, 1963
- Public Financial Institutions Act, 1983, (v) Consumer Protection Act, 1986
- The Credit Information Companies (Regulations) Act, 2005 and IT Act 2000
- However, recent IT (Amendment) Act, 2008, for the first time, introduces the concept of “sensitive personal information”, and fixes the liability of the ‘body corporate’ to protect the same. On the other hand, it helps to take legal action against an individual for the breach of confidentiality and privacy, under a lawful contract. The data protection regime in India emerges with these provisions.

- Compliance measures include:
 - Ethical Guidelines for Biomedical



Privacy provision in the Privacy Act may supersede all other privacy clauses which may be present in any other laws of the country

Research - Indian Council of Medical Research, 2000

- The Telecom Unsolicited Commercial Communication (UCC) Regulations, 2007, By TRAI
- Reserve Bank of India, Master Circular, July 2007

Presentation Sources

- **Kush Wadhwa**, Managing Director, Global Security Intelligence – Panel on Differences and Commonalities – Asia, Europe, and the U.S., September 2009
- **Kamlesh Bajaj**, CEO, Data Security Council of India (DSCI) - DSCI and Data Protection, September 2009
- Deliverable D2.1 – India Preparatory Meeting Report, RISE Workshop Report, October 2009
- **Dr. Kamlesh Bajaj**, (Data Security Council of India), Security and Privacy Challenges in the Unique Identification Project, March 2010
- **Mr. Vinayak Godse**, Director, Data Security Council of India, Data Security in E-Governance: Projects in India, December 2010

E-Governance in China



Industry Factsheet 4

Key facts about data privacy and biometrics in the PRC

- There is no unified data protection law.
- Some piecemeal developments include:
 - Amended PRC Criminal Law
 - Amended *Tort Law*
- Prediction: developments likely to be subject to State-wide security exceptions.
- The use of fingerprints in commercial and judicial practices has thousands of years history.
- Starting in 1990s there are 6 major centres for biometric R and D under the support of 863 and 973 focus programmes which funded by the Ministry of Science and Technology of China.
- At opening & closing ceremony of 2008 Beijing Olympic Game 100,000 audience passed 100 gates by speedy identity verification with facial recognition systems.
- There are 600,000 passengers who exit from or enter into Shenzhen customs per day. After using facial recognition devices, the time of customs checking per passenger is reduced from 13 seconds to 6 seconds.
- For improving the quality of training for novices and prevent fraud and "street killers", an intelligent driving training management system (biometric device) has been used in Suzhou City since 2008.
- There are near 200 enterprises which join the R&D and marketing of biometric products, and the output values in market is near CNY 300 millions *yuan*. China would be great market for biometric products and important provider of biometric technologies as well.

<p>Significant biometric applications in China</p>	<ul style="list-style-type: none"> • Governmental <ul style="list-style-type: none"> ○ Self-Service Border-crossing (deployed) <ul style="list-style-type: none"> – Shenzhen – Hong Kong Boarder since June 2005 – Zhuhai – Macau Boarder since April 2006 ○ Biometric E-Passport (on-going) • Enterprise: Time attendance and access control <ul style="list-style-type: none"> ○ Finger, Face, Iris, Palm • Consumer products <ul style="list-style-type: none"> ○ Face Logon – on notebook PC ○ Finger Logon – on mobile phone, PC ○ Finger Lock
<p>Foundations for enhancing ethical values for an e-society in the HKSAR</p>	<ul style="list-style-type: none"> • Legal Framework – Personal Data (Privacy) Ordinance & Electronic Transactions Ordinance • The eHealth Initiative – electronic health record (eHR) sharing infrastructure • Biometric applications and technologies • General guidelines to facilitate wider use of biometrics exist, but additional ones for specific use can be developed • Industry, academia and domain experts and regulatory bodies can collaborate on these
<p>Popular opinions in China for a good governance</p>	<ol style="list-style-type: none"> 1. Develop (pollute) first, and govern second. 2. Scientists only concern R&D, government and enterprises only concern investment, the public only concern enjoyment/consumption, and the humanists /social scientists only concern comments with hindsight (马后炮). 3. Governance should accompany development at initial stage and all stakeholders including government, scientists, engineers, humanists and social scientists, lawyers, businessmen, and the public need engagement in the governance from the very beginning.

Presentation Sources

- **Xiaomei Zhai**, Center for Bioethics, Chinese Academy of Medical Sciences, Beijing, P. R. China, 'The Status Quo and Ethical Governance in Biometric in Mainland China', January 2010

Privacy Impact Assessments



Industry Factsheet 5

The importance of security risk assessments and privacy impact assessments

How to more effectively use/deploy biometrics:

- Fundamental respect for privacy designed into products, systems and solutions
- Better informed users and customers
- Better industry “norms”
- Better integration among systems, toolkits, processes and management practices
- More explicit but “business-friendly” guidelines and regulatory regimes
- Explicit and early conduct of Privacy Impact Assessments and Security Risk Assessments

AICPA/CICA* privacy framework components

*American Institute of
Certified Public
Accountants/ Canadian
Institute of Chartered
Accountants

1. **Management**—Firms need to define, document, and communicate accountability for their privacy policies and procedures.
2. **Notice**—Firms need to provide notice about their privacy procedures and describe the purpose of collecting, using, retaining, and disclosing personal information.
3. **Choice and Consent**—Firms need to describe the choices available to people and obtain implicit or explicit consent for the use and disclosure of personal information.
4. **Collection**—Firms should collect information for the purposes identified in the notice.
5. **Use and Retention**—Firms should limit the use of personal information to the purpose specified in the privacy notice and for which the person has given implicit or explicit consent.
6. **Access**—Firms should provide people with access to their personal information for review and update.
7. **Disclosure to Third Parties**—Firms should only disclose personal information to third parties for the purposes specified in the privacy notice with the implicit or explicit consent of the person.
8. **Security**—Firms should protect personal information against unauthorized access, both physical and logical.
9. **Quality**—Firms should maintain accurate, complete, and relevant personal information for the purposes specified in the privacy notice.
10. **Monitoring and Enforcement**—Firms should monitor compliance with privacy policies and procedures and have procedures in place to address privacy inquiries and disputes.

12 Principles of DSCI Privacy Framework

- 1 Preventing Data Misuse
- 2 Notice
- 3 Choice and Consent
- 4 Collection Limitation
- 5 Accuracy
- 6 Use and Retention
- 7 Access and Correction
- 8 Disclosure to third parties
- 9 Security
- 10 Monitoring and Enforcement
- 11 Regulatory Compliance
- 12 Accountability

Privacy
Principles

Presentation Sources

- **Nandita Jain Mahajan**, Chief Privacy & Information Security Officer, IBM India/South Asia and Nalini K. Ratha Ph.D., Research Staff Member, Exploratory Computer Vision Group, IBM T.J. Watson Research Center - Biometrics in IT/ITes Organizations: Application, Challenges, and Recent Research, September 2009
- **Kush Wadhwa**, Managing Director, Global Security Intelligence, Privacy Impact Assessments: Impact on Security and Surveillance Technologies, May 2010