



# RISE Toolkits for Policy Makers

## 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 Policy: 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](http://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 policy implications of biometric technology:

Policy Challenges, Goals and Objectives.....	Page 3
Data and Identity Protection as Related to Policy .....	Page 5
E-Passport and Visa Systems.....	Page 6
Policy Guidelines .....	Page 8
Policy and Ethics .....	Page 11

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

# Policy Challenges, Goals and Objectives



Policy Factsheet 1

## Sources of Public Policy

- Member States
- EU, Commission and Parliament
- European Court of Human Rights
- Statutory, non-statutory regulatory bodies at different levels.
- Need to acknowledge the broad range of potential stakeholders influencing or influenced by these policy sources.

## Policy Challenges

- Sources of policy are not often in unison, ranging from complete opposition through to hidden tensions. Arguably Security policy is an area where divisions are even more pronounced.
- Sources of policy are often bypassed, excluded (EDPS).
- The inclusion of stakeholders from the setting of policy. Encourage stakeholder involvement and create a framework for dialog between the sources of policy.
- The main challenge is how to promote mobility, at the same time minimizing the risks to our security and privacy.
- Raising the awareness of the potential risks.
- Decision-making about prevention of risks, at the same maintaining public trust.
- Increasingly European Public administrations are offering their services online to businesses and citizens. Increasing risks that these services are developed as “stand alone” solutions just for the regional/national level and cannot interact with other services on European level.
- New eBarriers might emerge, impeding the proper functioning of the Internal Market.

## When Does Policy Fail?

- Policy direction has dangerous ramifications for individuals and social interactions with biometric technologies.
- Policies are polarizing.
- Policies are discriminatory and racist.
- Policies are technologically centric.
- The policy process is closed off to or open only to vested interests.
- Policies are short term, ill conceived, poorly executed, and reactionary.

## Policy Goals and Objectives

- Data protection is a fundamental right - as clearly stated in the EU Charter - and governments are accountable for ensuring effective protection of this fundamental right. The Lisbon Treaty confirms this. It mandates the Council and the European Parliament to adopt consistent legislation on data protection.
- Governments also must be accountable for what they do with the personal data which they use for the different public interests they serve. This varies from the use of data as a support of policies in areas like public health, transport or taxation, to publication of some personal data on the internet for reasons of transparency, or to surveillance of certain individuals for law enforcement purposes.
- Promote and support interoperability at all levels of European Public Administration.
- The existence of data protection authorities endowed with strong powers and competences becomes important for the individual. In particular, since the most vulnerable people in society (e.g. asylum seekers, beneficiaries of social help) are highly dependent on government, protective legislation and effective data protection authorities are a vital equaliser in this relationship.
- We need an ethical framework for evaluating any conduct which will be taken in biometrics R&D and its application. This framework will be formed by a set of principles of ethical governance, the set of principles is also core values shared and committed by stakeholders who engage in biometrics R&D and its application.

### Presentation Sources

- **Dr. Paul McCarthy**, 'Models of Policy Making', November 2009
- **Dr. Paul McCarthy**, Cesagen, Lancaster University, Individual Identity and International Perspectives on Biometrics, December 2010
- **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'

# Data and Identity Protection as Related to Policy



Policy Factsheet 2

## Key Facts from the European Interoperability (eID) Study, 2009

### Identity resources

- 13/32 countries (40.5%) are deploying eID cards
  - Including 6 countries relying private sector issued eID cards
  - Including 7 countries with eID cards deployed by public bodies.
- 12 countries currently have paper ID cards.
- 5 countries currently do not issue identity cards (all but one have eID plans)
- 5 countries are using biometrics
  - Countries are relying on fingerprint data
  - 21 countries have not made any plans for biometrics yet (66%).
  - biometric data not reported as an authentication method for specific eGovernment applications in any country
- 6 countries have mobile phone based identification solutions
- 21 countries have no plans for mobile phone based identification

### Analysis

- 27/32 countries (84%) use PKI systems
- 21 countries (66%) use user name/password systems:
- 18 countries (56%) have some form of multilevel authentication policy, only 5 have formally adopted
- Only 2 countries have a specific legal framework with regard to entity authentication

### Challenges

- Cross border use of national eIDs:
  - Can users be uniquely identified, other than by relying on national identity numbers which may not be re-usable at the cross border level for legal reasons?
  - Is a commonly agreed European level authentication assurance policy feasible?

### **Presentation Sources**

- **John Stienen**, (DG Informatics, European e-Government Services (IDABC)), Interoperable Delivery of European e-Government Services: Main Challenges, March 2010

# E-Passport and Visa Systems



Policy Factsheet 3

## EU Border Control: EU COMM Initiatives

- Objective
  - Fight against illegal immigration balanced with border crossing facilitation
- Means/schemes
  - SIS (SIS II) – law enforcement (judicial orders)/watchlist
  - VIS
    - to be fully operational at all border crossing points by 2013 – system should be online by Sept. 2010 – POSTPONED TWICE!
    - only for third country visa holders (TCNVH) (fingerprints)
  - new technologies (BIOMETRICS) for more efficient border management

## Future Initiatives

- Registered Travelers (RT)
  - pre-enrolled, pre-vetted
  - mutual recognition (bilateral) between S and non-S countries
  - possibly using same e-gates as for ABC
  - use of e-passport? Face and fingerprints?
- Entry/Exit
  - Registration of entry/exit of third country nationals (with or without visa) using biometric identifiers (face, fingerprints?) to avoid overstayers.
- ESTA
  - pre-departure travel authorization for third country nationals not requiring visa (TCNVE).
- ABC
  - no enrolment, with e-passport.
  - only for EU citizens within “Schengen”
  - in accordance with SBC: minimal first line checks + random second line
  - not part of EC policy

## Legal Base for EU Border Checks

- Regulation (EC) No 562/2006 of 15 March 2006: the Schengen Borders Code (SBC)
- Complicating factor:
  - Not all EU Member States apply the SBC (ex. UK)
  - Some non-EU Member States do (ex. CH).
- Different entry/exit border control requirements for different nationalities
  - EU nationals vs. non EU nationals
  - art. 7 SBC
  - TCN enjoying the right of free movement, TCNVH, TCNVE



- different procedures + different role of biometrics in the border control process
  - identification, verification, authentication
  - security, efficiency, convenience

## Visa Information System (Schengen area) - Facts, Figures and Impacts

Visa Information System (relating to the introduction of biometric data for visas in the Schengen area):

- Biometrics are stored for 5 years and not re-taken for subsequent requests within a period of 59 months
- Applicants are obliged to appear personally to give fingerprints and have picture taken (live), at least the first time
- Introducing fingerprints adds considerable time (5 min per applicant) in the consulate
- Only very limited categories of persons are exempt from fingerprinting
  - Children < 12 years (awaiting study results, < 6 years)
  - Heads of State
- At border-control, fingerprint verification will be mandatory (after transition period), also adding time to the process
- Fingerprints may be used for criminal background searches by host country
- Asylum seekers' fingerprints will be used to search the VIS

### Presentation Sources

- **Max Snijder** (CEO European Biometrics Group), 'Biometrics at EU Borders and Biometrics for Public Administration', November 2009

# Policy Guidelines



Policy Factsheet 4

## General Policy Guidelines

- Rule making should set guiding principles for privacy in line with the globally recognized privacy principles.
- Consult with and include all government agencies which collect, process, store, transfer, disclose and use personal information of the end users.
- Establish a national ecosystem that is continuously engaged for the data protection cause.
- Foster collaboration and partnership with all stakeholders including private sector for promotion of this cause.
- Dedicate sufficient resources and investment on technology research, for promoting academic projects, and creating an infrastructure for this cause.
- Focus on awareness and education of the end users.
- Issue guidelines and standards that provide practical guide government departments, e-Governance projects and private sectors.
- Establish a mechanism for data breach notifications that mandates organizations to report the data breaches.

## E-Governance Policy Guidelines

- Revisit design, architecture, and deployment of projects from privacy perspective. Conduct routine privacy impact assessments.
- 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.
- Implement adequate measures for security and vulnerability management of systems that engage in processing of personal information.
- Build an organization culture that respects privacy of the end users.
- Ensure that privacy policies and practices are defined and implemented.
- Ensure that significant effort is dedicated on end user's education that enables them to take trust decisions while they are transacting online.
- Establish vigilant monitoring for privacy; deploy a mechanism to address end user's grievances.

## Policy Making for Identity Management: Questions to Ask

- Who should decide where and how biometrics shall be implemented?
- Who should participate in these discussions and where, in order to make the difference in existing policies?
- How can the identity management policy promote the opportunity for citizens to interact with government digitally but at the same time maintain their security and privacy?
- What kind of solutions are there for interoperability problems that are challenging the pan-European crossborder services?
- What are policies and technologies to assure the identity and security of the whole process, especially the flow of personal data?
- What kind of principles and guidelines could help service providers in designing the processes and technologies?
- What should we do in order to promote the “built-in privacy” technologies?
- Which identity tokens are reliable in the digital world, which are less controlled and supervised?

## Protecting Fundamental Rights, Privacy and Security: Questions to Ask for New Technologies

- When implementing new technologies, what kind of mechanisms could help us address the very complex issues of protecting the fundamental rights of citizens?
- How do we support the deliberation of the values at stake and the ways in which we apply them during the decision and technology development processes?
- What further analysis is needed on the ethical and social impact of the developed processes and technologies?
- How do we find a proper balance between the individual rights and the public good?
- As a result of the new technology, will there be a dramatic change in our societal relations and attitudes?
- Who will assess the broader ethical and societal impact of those technologies?
- Who should be involved in those decisions, or at least in consultancy process, how to engage the civil society?
- How can we raise awareness of all stakeholders and user-groups?
- How can we ensure that the principles for data protection will be applied in an effective manner?
- Do we need to review the current legislative framework?
- What kind of guidelines do we need to create for ensuring the privacy built-in and inclusive designs of systems?

### Presentation Sources

- **Data Security Council of India**, Marg, New Delhi, 'RISE Project Policy Paper: Policy in India', May 2010
- **RISE Stakeholder Workshop 2 Report**, D3.2, April 2010

# Policy and Ethics



Policy Factsheet 5

## Guidelines for the Governance of New Technologies

- New decisions on policy within security settings must be supported by a global dialog, which must be ethically informed.
- It is important that conversation between stakeholders, international actors and policy makers is ongoing and sustained.
- Policy makers must organize collective responsibility of both intended and unintended consequences.
- Societal intervention must take place early in the RTD process.
- Adopt the participatory approach of “user-involvement” when designing new technology.
- Consider ethics-privacy requirements not as constraints but as constructive drivers of innovation.
- Promote public debate wherever appropriate (especially on the issue of proportionality of impact on privacy and data protection).

## Cyber-Security: Ethical Issues

- We must find ways to balance the security and civil liberties and to find the balance between the control-state and the unlimited-state in order to ensure the security to its citizens.
- We must determine to what extent the government should control or trust the basic infrastructure service providers in the democratic states.
- We have to think much more about the risks accompanied to the actions taken in response to the citizens’ strong demand for security and transparency
- Democracy of the state is based on the ideal of transparency, but the demand of total transparency may destroy the delicate balance necessary to maintain it.
- When developing secure environments against different threats from cyberspace, we must understand and balance the costs and the acceptable risks.

### Presentation Sources

- **RISE Stakeholder Workshop 2 Report**, D3.2, April 2010
- **Dr. René von Schomberg**, RISE Project, European Commission Research DG, Governance and Ethics Unit, Research on Ethics/Governance under the Science in Society Programme, December 2010
- **Mr Jaak Aaviksoo**, Estonian Minister of Defence, Are Democratic States More Vulnerable to Cyberterrorism?, March 2010
- **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, 8<sup>th</sup> Summer School for advanced studies on biometrics for secure authentication - Alghero 10<sup>th</sup> June 2011