Privacy by design?

The case of biometrics

PrimeLife/IFIP Summer School 2009
Els Kindt, Legal Researcher, K.U. Leuven – ICRI
Introduction

Theme of PrimeLife/IFIP Summer School 2009

‘privacy and identity management for emerging internet applications throughout a person's life’

Biometrics: advantages and disadvantages

- Link person - identity in online/offline situations (authentication)
- Risks of abuse (re-use of data for other purposes)
- Risks of theft
- ...

Question: Is there a ‘safe’ way of using biometrics?

PrimeLife/IFIP Summer School 2009
Overview

1. Issues inherent to the use of biometrics in identity management

2. Solution: privacy by design?
   definition?
   how?
   solutions by Turbine

3. Towards best practices
1. Issues inherent to the use of biometrics

**Advantages of biometric data**

- Enhances authentication means / security
  E.g., password management, control of restricted access
  Creates link between real and virtual world

- Ability to verify if holder of document is person to whom document is issued

- Ability to identify individuals
  E.g., if no other means available

- Convenience
1. Issues inherent to the use of biometrics

Privacy risks for the data subject

- **Unique**
  - Theft
  - Unique identifier: linking of information
- ‘Sensitive’ information
  - Health related information
- Re-use
  - E.g., Eurodac
- Permits identification
1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics:
many open legal issues

- Biometrics: problems with legal definitions
  
  • Are biometric data personal data which are subject to the Data Protection Directive 95/46/EC?
1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics:

many open legal issues

- Are biometric data personal data?

Distinction between ‘images’ and ‘templates’
1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics: many open legal issues

- Are biometric data personal data?

Recital 26 of the Data Protection Directive 95/46/EC:

‘(...) whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person: (...)’ (emphasis added)
1. Issues inherent to the use of biometrics

“measures of biometric identification or their digital translation in a template form in most cases are personal data”

Art. 29 WP Working document on biometrics, adopted 1 August 2003

But:

Exception: in case templates would be stored in such a way that (1) no reasonable means can be used by (2) the controller or (3) by any other person to identify the data subject

Different implementation and interpretation in the Member States, e.g., United Kingdom

Local storage on card: could be considered as ‘private use’?
1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics: many open legal issues

- Biometrics: problems with legal definitions
  - Are biometric data sensitive data?
  - Which personal data are biometric data?
    - e.g., digital picture?
    - cfr. France, the Netherlands
  - Quid ‘protected templates’?
1. Issues inherent to the use of biometrics

**EU Legal & Regulatory Framework for Biometrics:**
many open legal issues

- May biometric data be centrally stored?
- Which human characteristics shall be used?
- What security measures shall be applied?
- ...

Few national laws of EU Member States explicitly regulate the use of biometrics

Exceptions: E.g., France: Modification of 6 August 2004 of Law N°78/17 of 6.01.1978 but: limited
1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics
Preliminary conclusion:

(1) Biometric applications process (in most cases) personal data
   • Inherent to biometric applications: used to identify/authenticate the identity of a person
   • Confirmed in opinion Art. 29 WP on personal data 2007

(2) Data Protection Directive 95/46/EC (national laws) will apply
   • To processing by companies in EU, or
   • If equipment is used on territory of EU Member States
     – Except for transit only

(3) Fundamental Right to privacy involved (art. 8 ECHR)
2. Solution : privacy by design ?

Concept of ‘Privacy by design’

– Ontario’s Privacy Commissioner, Dr. Ann Cavoukian, back in the 90’s
– Stresses concept as an organization’s default’s way of operating

• Privacy is embedded in the design
• Visibility and transparency
• Respect for user privacy

– Objectives : ensuring privacy and personal control over one’s information

– See http://www.privacybydesign.ca/
2. Solution: privacy by design?

Concept of ‘Privacy by design’

– **Dutch Data Protection Authority stresses**
  - Protection of personal data
  - Review of need of identification versus anonymity (e.g. of clients)
  - ‘Less is more’ concept
  - Control of access


– **PETs** (Borking)
  - Tools for realisation of privacy by design (more narrow)
  - Dutch Ministry of the Interior: ‘PETs. Whitepaper for decision makers’
  - See COM/2007/0228final: ‘breaches of data protection technically more difficult’; ‘eliminating/reducing personal data’
## 2. Solution: privacy by design?

What does it mean for biometrics?

<table>
<thead>
<tr>
<th>Risks</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique</td>
<td>Context dependent use of biometrics</td>
</tr>
<tr>
<td>• Theft</td>
<td>• revocability</td>
</tr>
<tr>
<td>• Unique identifier: linking of information</td>
<td>• Transformation and pseudonymity</td>
</tr>
<tr>
<td>‘Sensitive’ information</td>
<td>Excluding use of ‘sensitive’ data and irreversibility</td>
</tr>
<tr>
<td>• Health related information</td>
<td>• Linking use to specific service context and pseudonymity</td>
</tr>
<tr>
<td>Re-use</td>
<td>• Local storage and verification functionality</td>
</tr>
<tr>
<td>• E.g., Eurodac</td>
<td></td>
</tr>
<tr>
<td>Permits identification</td>
<td></td>
</tr>
</tbody>
</table>
2. Solution: privacy by design?

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Turbine design: use of protected templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Context dependent use of biometrics</td>
<td></td>
</tr>
<tr>
<td>• revocability</td>
<td></td>
</tr>
<tr>
<td>• Transformation and pseudonimity</td>
<td></td>
</tr>
<tr>
<td>• Excluding use of ‘sensitive’ data and irreversibility</td>
<td></td>
</tr>
<tr>
<td>• Very limited biometric data (Auxiliary data (AD)) is used</td>
<td></td>
</tr>
<tr>
<td>• for issuance of multiple pseudo-identities (PIs) (diversification)</td>
<td></td>
</tr>
<tr>
<td>• for renewable templates which can be revoked</td>
<td></td>
</tr>
<tr>
<td>• ‘raw’ data and templates: deleted after extraction and PIs nor AD can be reversed to such data</td>
<td></td>
</tr>
</tbody>
</table>
2. Solution: privacy by design?

Objectives

- Pseudonymity and preventing database crossmatching
- Local storage and verification functionality

Turbine design: use of protected templates

- Independent Pseudonyms (PIs) are linked to specific service provider
- Storage of PIs and ADs separately and on token
2. Solution: privacy by design?
Architectures for Pseudo identity management

Supplementary data (SD) can be used for security enhancement by:
- possession or knowledge-based secrets
- service specific secrets or signatures
- PI validity data
- digital signature or certification of data

Storage and computations can be local (token, sensor), central (server, database) or shared
2. Solution: privacy by design?

Proposed ‘Privacy by design’ for biometrics and existing data protection regulation

**Turbine design**

- **issuance of multiple pseudo-identities (PIs) (diversification)**

- **renewable** templates which can be revoked

- ‘raw’ data and templates: deleted after extraction and PIs nor AD can be reversed to such data

- **Data minimisation** (Directive 95/46/EC)

- Risks of theft (Working document on biometrics of article 29 Working Party (1 August 2003))

- Prohibition of processing of sensitive data (Directive 95/46/EC)
### Proposed ‘Privacy by design’ for biometrics and existing data protection regulation

#### Turbine design

<table>
<thead>
<tr>
<th>Independent Pseudonyms (PIs) are linked to specific service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage of PIs and ADs separately and on token</td>
</tr>
</tbody>
</table>

#### Risks of unique identifiers and cross linking (Working document on biometrics of article 29 Working Party (1 August 2003)) and specification of purpose principle (Directive 95/46/EC)

- Purpose limitation but no specific storage requirements (Directive 95/46/EC)
2. Solution: privacy by design?

Comparison with PrimeLife objectives?

- Use of multiple pseudonyms which are unlinkable (data minimisation)

- User control and consent

- Transparancy for the data subsubject

2. Solution: privacy by design?

But:

Only partial technical measures which improve protection against privacy risks

Does not replace:
- all technical measures which may be (legally) required and appropriate e.g., access control
- all appropriate organizational measures e.g., confidentiality clauses, education, …
- alternative means e.g., right to appeal at no cost
- appropriate legal regulation e.g., no covert collection, …
2. Solution: privacy by design?

and: unsolved: including

- Technical safeguards against remote and unobserved collection and use if reference biometric data (e.g., fingerprint and/or face) are stored centrally
  - Need for regulation?

- Deployment in environments with multilateral security (who is in control) lacking user control (e.g., use of EU passports in the U.S.)

- Typical error rates (FAR, FRR, …)
3. Towards best practices


List of best practices

- organizational
- legal compliance
- some technical means

Should be updated
3. Towards best practices

See also
European Privacy and Data Protection Commissioners

Encourage the development and improvement of comprehensive data protection legislation

That (...) encourage organisations to adopt best practices, including privacy by design; (...)

*Declaration on leadership and the future of data protection in Europe*, Edinburgh, 23-24 April 2009
3. Towards best practices

Suggested Best Practices for use of biometrics in private sector

- No storage of ‘raw images’ (deletion)
  cfr Opinions of DPAs; findings of study 'Biometrics as a PET' in the Netherlands
- Decentralisation
- Use of verification function only
  Prohibition to use central databases? Exceptions?
- Distinct use in private and public sector
- Transparency to the data subject
- Specific security measures
  limited access, encryption, deletion policy, …
3. Towards best practices

And:

- ‘Anonymous use’ and/or use of various ‘identities’ (pID) (pseudonyms) where possible
- Use of irreversible templates
- Unlinkability of templates
- Revocability
- Considerable degree of control by the data subject
- …
3. Towards best practices

Especially biometric data processing

Insufficient/inadequate legislation

privacy enhancing technologies / best practices

Need to impose PETs /best practices by regulation ?
See also Art. 27 Directive 95/46/EC

‘(…) encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions (…) taking account of the specific features of the various sectors’

- Directed towards trade associations/bodies representing categories of controllers
- National level
- Community code
Conclusion

Theme of PrimeLife/IFIP Summer School 2009

`privacy and identity management for emerging internet applications throughout a person's life`?

Especially biometric data processing requires

`Privacy by design`
Conclusion

‘Privacy by design’

Providing revocable biometric identifiers, unlinkable and irreversible and under the control of the data subject
Conclusion

Especially biometric data processing requires ‘Privacy by design’

 goes ‘hand in hand’ with

appropriate organisational measures, legal compliance and adequate legal regulation of biometrics


European Commission, *Communication on Promoting Data Protection by Privacy Enhancing Technologies (TETs)*, COM/2007/0228final

