Privacy, Security and facial deidentification aspects

By
Mickey Cohen, CEO
Shanit Ltd
Mickey@shanit.co.il
+972-54-758-6312
Presentation layout

- SC27/WG5 Identity management and privacy technologies (ISO/IEC 20889, 27552)
- SC27 IT Security techniques (ISO 27xxx)
- Practical workflows and privacy
- Examples
- Summary
ISO 27552 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

<table>
<thead>
<tr>
<th>Application areas</th>
<th>Smart cities</th>
<th>Internet of Things</th>
<th>Big Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminology and principles</td>
<td>27570</td>
<td>27030</td>
<td>20547-4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General framework</th>
<th>Privacy references list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminology and principles</td>
<td>Privacy references list</td>
</tr>
<tr>
<td>29100</td>
<td>SD2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management</th>
<th>Privacy impact assessment</th>
<th>Extension to ISMS for privacy management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminology and principles</td>
<td>29134</td>
<td>27552</td>
</tr>
<tr>
<td>29151</td>
<td>PID controls</td>
<td>Requirements &amp; Guidelines</td>
</tr>
<tr>
<td>27001/2</td>
<td>Controls</td>
<td></td>
</tr>
<tr>
<td>27018</td>
<td>Cloud Controls</td>
<td></td>
</tr>
<tr>
<td>NP 27555</td>
<td>Deletion</td>
<td></td>
</tr>
</tbody>
</table>

Freely available
ISO 20899 - Privacy enhancing data **de-identification** terminology and classification of techniques
Privacy and Security

• ISO/IEC 27522 maps Privacy Information Management System (PIMS) onto Information Security Management System (ISMS) so that Personally Identifiable Information (PII) can be addressed through a known framework.

• Security is a moving balance between Requirements, Threats, Usability and … Budgets.
ISO/IEC 27522

• Guidance for Privacy by Design (PdD)
• Limitations on collection, on processing, minimization, de-identification, deletion, end of processing, retention, disposal etc.
• Transfer and record of transfer of PII
• Addresses Controllers and Processors
• Relates closely with General Data Protection Regulation (GDPR)
ISO/IEC 20889 De-Identification

• Addresses de-identification of PII by removal of any possible link with a data subject (natural person) GDPR, HIPPA, COPA etc.
• Addresses risks of re-identification attacks
• Discusses de-identification techniques
• Addresses anonymization, pseudonymisation
• Suggests techniques such as noise, permutations, encryption, synthetic data
• Formal privacy measurement models
ISO/IEC 20889 De-Identification

No practical implementation or tool for de-identification is suggested
Privacy Risk over exposure time

Person in view

Take image (A)

Extract Template (B) and erase image (C)

Search (D) and erase Template

Identified

Process known person

Not Identified

Process person

Secured zone
handling time ~0.2s

Official enrollment (With consent and alternative)

Protected Biometric Database

VPN

Shanit
Privacy Risk and search space

- Images – more like blobs
- “Search space” 100 people
- Images kept for 20-30 seconds
- No real risk of identification

Is there a quality level below which privacy is a lesser issue? Is time a factor?
De-Identification

- Every database is destined to be breached.
- Many organizations need to keep facial images pending consent.
De-Identification - Solution

• Process images so that they are similar to humans and resist Face Recognition Technologies.
• Images displayed to officers or printed are only the De-Identified version.
Classic methods such as encryption, pixelation and blurring limit the use of the photo and does not fully protect against face recognition.
De-Identification
De-Identification

Biometric Data
De-Identification - Usage

- Cloud Storage
- Social Networks
- Financial Institutes
- Health Care
- Government & Security
Summary

• Same as security – Privacy is a moving target – **an ever evolving challenge**
• Short stay could be a low privacy risk
• Low quality could be a low privacy risk
• Long time storage – hi risk -> encryption and de-identification
Final Summary

Mickey Cohen
Mickey@shanit.co.il  +972-54-758-6312

Those wishing to receive their de-identified image may email.