IoT and Smart Cities: Personal Data Protection Strategies and Guidelines

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IOT4SCC: Joint Workshop on IoT for Smart Cities & Communities Platform Convergence: Breakout C, 7 June 2018
Outline on Session on Personal Data Protection Strategies and Guidelines

Session 1 (12.30 - 13.30)
• Citizen viewpoint for smart cities
  • Mara Balestrini, Ideas for change
• Privacy-by-design viewpoint for smart cities
  • Antonio Kung, Trialog
• Introduction to smart city use case session
• Selection of smart city use case

Session 2 (14.30-15.30)
• Practice / Legal and ethical compliance viewpoint for smart cities
  • Pasquale Annicchino, Archimede Solutions
• Smart city use case session
  • Breaches
  • Threats and consequences
  • Measures
• Conclusion
Citizen viewpoint for smart cities

Mara Balestrami, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Privacy-by-design Viewpoint for Smart Cities

Antonio Kung, Trialog, France

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Antonio Kung

- European projects: PRIPARE, Create-IoT...
- IPEN wiki (ipen.trialog.com)
- EIP-SCC Citizen approach to data: privacy-by-design
  - Workshop London (March 2017)
  - Workshop Milan (July 2017)
  - Workshop Brussels – Eurocities (January 2018)
- Involved in standardisation
  - ISO/IEC 27570 - Privacy guidelines for smart cities
  - ISO/IEC 27030 - Security and privacy guidelines for IoT
  - ISO/IEC 27550 - Privacy engineering for system life cycle processes
  - ISO/IEC 30147 - Methodology for implementing and maintaining trustworthiness of IoT systems and services
  - ISO/IEC 20547-4 – Big data reference architecture – Security and privacy
ICT Trend towards Complex Ecosystems

Ecosystems:
- Smart Cities
- IoT
- Big data

Domains:
- Ecosystems
- Smart grid
- Health
- Transport

Concerns:
- Security
- Safety
- Privacy
Smart Cities Deal with Ecosystems

- **Co-funded by the European Commission**

**Municipality stakeholder**

- **Requests**
  - **Agreements**
  - **For data exchange**

- **Contracts**

**PIA**

- **Give consent**
  - **Agree**
  - **Comply**

**Data Controller**

- **Integrator**
  - **Apply**

**Supplier**

- **Citizen**
  - **Privacy Obligations**
  - **PIA and PbD**
  - **Purpose known**
  - **Requirements Purpose unknown**

- **Give consent**
  - **Agree**
  - **Apply**

- **Give consent**
  - **Agree**
  - **Apply**
Ecosystems Involve Supply Chains

Operator
Application 1

Operator
Application 2

Integrator

Supplier

Sensor
Smart device
Cloud solution
Electronics
Security module
OS
Middleware

Supply Chain

Co-funded by the European Commission
Example of Big Data Ecosystem: AutoMat

- OEM Backend
  - Storing data in the cloud
  - Data access
  - Combining and enriching data
  - Pre-processing and aggregation
  - Data acquisition contract
  - Car data capturing

- Marketplace
  - Data access clearance
  - Apps and services publishing

- Service providers
  - B2C Services & App Stores
  - B2B Service provision

- Users
  - Vehicle Users
  - Service Consumers

- Storage provider
  - Automotive manufacturer

- Other data sources
  - Combining and enriching data

Co-funded by the European Commission
Need to coordinate between ecosystem stakeholders

- Example of coordination needs
  - Privacy compliance
    - Global privacy impact assessment vs organisation PIA
    - PII tracking e.g. upon user consent removal
  - Data breach management
  - Cybersecurity compliance
    - Global risk analysis vs organisation risk analysis
    - Cybersecurity incident management
Impact on Standards Landscape

Additional guidelines
For ecosystems

Privacy Standards for Smart Cities
27570 Privacy guidelines

Privacy Standards for Big Data
20546-4 Security and privacy

Privacy Standards for IoT
27030 Security and privacy guidelines

General Privacy Standards
Privacy framework 29100
Privacy impact assessment 29134
Privacy engineering 27550
Code of practice 29151
Privacy Information management systems 27552
OASIS-PMRM
Thank You!

The CREATE-IoT project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com
Introduction to smart city use case session

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Context

• Many such sessions carried out since 2017
• Participative approach
  • Citizen, Policy makers, Engineers
• Templates based on standards
• Content : impact analysis
  • Breaches
  • Threats and consequences
  • Measures
Security and privacy assessment (based on ISO/IEC 27550)

Threats
- Focus on privacy
  - Vulnerability of data processing
- Focus on security
  - Vulnerability of the system

Breach

Consequences (or impact, or severity)
- Privacy for Citizen
- Organisational

Measures
- Organisation
- Technical
## Risk map (based on CNIL guidelines)

<table>
<thead>
<tr>
<th>Threat Likelihood</th>
<th>Impact Likelihood</th>
<th>Must be avoided or reduced</th>
<th>Must be reduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Impact</td>
<td>Maximum Impact</td>
<td><strong>Absolutely avoided or reduced</strong></td>
<td><strong>A</strong></td>
</tr>
<tr>
<td>Significant Impact</td>
<td>Significant Impact</td>
<td><strong>These risks may be taken</strong></td>
<td><strong>O</strong></td>
</tr>
<tr>
<td>Limited Impact</td>
<td>Limited Impact</td>
<td><strong>Must be reduced</strong></td>
<td></td>
</tr>
<tr>
<td>Negligible Impact</td>
<td>Negligible Impact</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Example

- **Breach:** Alice attendance to an Alcoholics Anonymous meeting is made public

- **Threat and consequence**
  - **Threat:** Some one hacks into the attendance management system and retrieves the log of attendance
  - **Consequence**
    - **Likelihood significant**
    - **Impact**
      - for Alice could be maximum
      - For the organisation could be significant

---

**Likelihood:**
- **Negligible**
- **Limited**
- **Significant**
- **Maximum**
## Threats (based on LINDDUN and STRIDE)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linkability</td>
<td>Unlinkability</td>
</tr>
<tr>
<td>Identifiability</td>
<td>Anonymity</td>
</tr>
<tr>
<td><strong>Non-repudiation</strong></td>
<td>Plausible deniability</td>
</tr>
<tr>
<td>Detectability</td>
<td>Undetectability and unobservability</td>
</tr>
<tr>
<td>Disclosure of information</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Unawareness</td>
<td>Content awareness</td>
</tr>
<tr>
<td><strong>Non compliance</strong></td>
<td>Policy and consent compliance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
</tr>
<tr>
<td>Tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td><strong>Repudiation</strong></td>
<td>Nonrepudiation</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Denial Of Service</td>
<td>Availability</td>
</tr>
<tr>
<td><strong>Elevation of privilege</strong></td>
<td>Authorization</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-categories</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policies</td>
<td>Management direction</td>
</tr>
<tr>
<td>Organization</td>
<td>Internal organisation</td>
</tr>
<tr>
<td></td>
<td>Mobile devices and teleworking</td>
</tr>
<tr>
<td>Human resource security</td>
<td>Prior to employment</td>
</tr>
<tr>
<td></td>
<td>During employment</td>
</tr>
<tr>
<td></td>
<td>Termination and change of employment</td>
</tr>
<tr>
<td>Asset management</td>
<td>Responsibility for assets</td>
</tr>
<tr>
<td></td>
<td>Information classification</td>
</tr>
<tr>
<td>Access control</td>
<td>Business requirements of access control</td>
</tr>
<tr>
<td></td>
<td>User access management</td>
</tr>
<tr>
<td></td>
<td>User responsibilities</td>
</tr>
<tr>
<td></td>
<td>System and application access control</td>
</tr>
<tr>
<td></td>
<td>Media handling</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Cryptographic controls</td>
</tr>
<tr>
<td>Physical and environmental security</td>
<td>Secure areas</td>
</tr>
<tr>
<td></td>
<td>Equipment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation security</td>
<td>Operational procedures and responsibilities</td>
</tr>
<tr>
<td></td>
<td>Protection from malware</td>
</tr>
<tr>
<td></td>
<td>Backup</td>
</tr>
<tr>
<td></td>
<td>Logging and monitoring</td>
</tr>
<tr>
<td></td>
<td>Control of operational software</td>
</tr>
<tr>
<td></td>
<td>Technical vulnerability management</td>
</tr>
<tr>
<td></td>
<td>Information systems audit considerations</td>
</tr>
<tr>
<td>Communication security</td>
<td>Network security management</td>
</tr>
<tr>
<td></td>
<td>Information transfer</td>
</tr>
<tr>
<td>System acquisition, development and maintenance</td>
<td>Security requirements</td>
</tr>
<tr>
<td></td>
<td>Security in development processes</td>
</tr>
<tr>
<td></td>
<td>Test data</td>
</tr>
<tr>
<td>Suppliers relationships</td>
<td>Security in supplier relationships</td>
</tr>
<tr>
<td></td>
<td>Supplier service delivery management</td>
</tr>
<tr>
<td>Incident management</td>
<td>Management of incidents and improvements</td>
</tr>
<tr>
<td>Business continuity</td>
<td>Information security continuity</td>
</tr>
<tr>
<td></td>
<td>Redundancies</td>
</tr>
<tr>
<td>Compliance</td>
<td>Compliance (legal and contractual)</td>
</tr>
<tr>
<td></td>
<td>Information security reviews</td>
</tr>
</tbody>
</table>
Privacy measures (based on ISO/IEC 27552)

<table>
<thead>
<tr>
<th>Category</th>
<th>Measures for Data Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions for collection</td>
<td>Identify and document purpose</td>
</tr>
<tr>
<td>and processing</td>
<td>Identify lawful basis</td>
</tr>
<tr>
<td></td>
<td>Determine when and how consent is to be obtained</td>
</tr>
<tr>
<td></td>
<td>Obtain and record consent</td>
</tr>
<tr>
<td></td>
<td>Privacy impact assessment</td>
</tr>
<tr>
<td></td>
<td>Contracts with PII processors</td>
</tr>
<tr>
<td></td>
<td>Records related to processing PII</td>
</tr>
<tr>
<td>Rights of PII principals</td>
<td>Determining PII principals rights and enabling exercise</td>
</tr>
<tr>
<td></td>
<td>Determining information for PII principals</td>
</tr>
<tr>
<td></td>
<td>Providing information for PII principals</td>
</tr>
<tr>
<td></td>
<td>Provide mechanism to modify of withdraw consent</td>
</tr>
<tr>
<td></td>
<td>Provide mechanism to object to processing</td>
</tr>
<tr>
<td></td>
<td>Sharing the exercising of PII principals</td>
</tr>
<tr>
<td></td>
<td>Correction or erasure</td>
</tr>
<tr>
<td></td>
<td>Providing copy of PII processed</td>
</tr>
<tr>
<td></td>
<td>Request management</td>
</tr>
<tr>
<td></td>
<td>Automated decision taking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Measures for Data Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions for collection</td>
<td>Cooperation agreement</td>
</tr>
<tr>
<td>and processing</td>
<td>Organization’s purposes</td>
</tr>
<tr>
<td></td>
<td>Marketing and advertising use</td>
</tr>
<tr>
<td></td>
<td>Infringing instruction</td>
</tr>
<tr>
<td></td>
<td>PII controller obligations</td>
</tr>
<tr>
<td>Rights of PII principals</td>
<td>Records related to processing PII</td>
</tr>
<tr>
<td></td>
<td>Obligations to PII principals</td>
</tr>
</tbody>
</table>
## Privacy measures (based on ISO/IEC 27552)

<table>
<thead>
<tr>
<th>Category</th>
<th>Measures for Data Controllers</th>
<th>Category</th>
<th>Measures for Data Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy-by-design and by-default</strong></td>
<td>Limit collection</td>
<td><strong>Privacy-by-design and by-default</strong></td>
<td>Temporary files</td>
</tr>
<tr>
<td></td>
<td>Limit processing</td>
<td></td>
<td>Return transfer or disposal of PII</td>
</tr>
<tr>
<td></td>
<td>Define and document PII minization and de-identification objectives</td>
<td></td>
<td>PII transmission controls</td>
</tr>
<tr>
<td></td>
<td>Comply with data minimization and de-identification use</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PII de-identification and deletion</td>
<td><strong>PII sharing, transfer and disclosure</strong></td>
<td>Basis for transfer of PII</td>
</tr>
<tr>
<td></td>
<td>Temporary files</td>
<td></td>
<td>Countries and organisations to which PII might be transferred</td>
</tr>
<tr>
<td></td>
<td>Retention</td>
<td></td>
<td>Records of PII disclosure to third parties</td>
</tr>
<tr>
<td></td>
<td>Disposal</td>
<td></td>
<td>Notification of PII disclosure requests</td>
</tr>
<tr>
<td></td>
<td>Collection procedures</td>
<td></td>
<td>Legally binding PII disclosures</td>
</tr>
<tr>
<td></td>
<td>PII transmission controls</td>
<td></td>
<td>Disclosure of subcontractors used to process PII</td>
</tr>
<tr>
<td><strong>PII sharing, transfer and disclosure</strong></td>
<td>Identify basis for PII transfer</td>
<td></td>
<td>Change of subcontractor to process PII</td>
</tr>
<tr>
<td></td>
<td>Countries and organisations to which PII might be transferred</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Records of transfer of PII</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Records of PII disclosure to third parties</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Joint controller</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table above lists various privacy measures based on ISO/IEC 27552, categorized into 'Privacy-by-design and by-default' and 'PII sharing, transfer and disclosure'. Each category includes specific measures such as limiting collection, defining and document PII minimization, and identifying the basis for PII transfer among others.
The five Results of a Workshop

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[5] Conclusions / Actions</td>
<td></td>
</tr>
</tbody>
</table>
Example: open data

- Organisational Layer
- Function & service Layer
- Information Layer
- Communication Layer
- Component Layer

<table>
<thead>
<tr>
<th>Open data</th>
<th>Anonymisation</th>
<th>Data set</th>
<th>Aggregation</th>
<th>Data</th>
</tr>
</thead>
</table>

- External perimeter
- Community perimeter
- Personal perimeter

- Market integration
- Business integration
- External Data processing
- Internal Data processing
- Near-field interaction
- Environmental interaction
Thank You!

The CREATE-IoT project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com

Co-funded by the European Commission
Selection of Use Case

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Use case

• Open data
  • Data collected from citizen activities (e.g. smart phones)
  • Data aggregated and anonymised by smart city service

• Other use case
  • Bike sharing application based on smart phone
  • Service provider wishes to trade collected data (e.g. status of road)
  • Specific IoT devices added for instance RFID sensors
Legal and Ethical Compliance Viewpoint for Smart Cities

Pasquale Annicchino, Archimede Solutions, Switzerland

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Smart city use case session: Breaches

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Open Data Breaches

- Massive personal data leak
- Massive business data leak
- Fake data

![Diagram]

- Market integration
- Business integration
- External Data processing
- Internal Data processing
- Near-field interaction
- Environmental interaction

- Open data
- Anonymisation
- Data set
- Aggregation
- Data
- Collection

External perimeter | Community perimeter | Personal perimeter
Bike Sharing Breaches

- Massive personal data leaks
- Injecting fake data
- Manipulation of data to get commercial advantage
- Misuse of the location of individual data
Smart city use case session: Threats and Consequences

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Open Data Threat and Consequences

- Massive privacy leak
  - Weak anonymization
- Massive business data leak
- Fake data

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>Maximum</td>
<td>Absolutely avoided or reduced</td>
</tr>
<tr>
<td>Significant</td>
<td>Limited</td>
<td>Must be avoided or reduced</td>
</tr>
<tr>
<td>Limited</td>
<td>Negligible</td>
<td>These risks may be taken</td>
</tr>
<tr>
<td>Negligible</td>
<td>Limited</td>
<td>Must be reduced</td>
</tr>
</tbody>
</table>

Co-funded by the European Commission
Bike Sharing Threat and Consequences

- Massive personal data leaks
- Injecting fake data
  - Using bikes to simulate bumps
- Manipulation of data to get commercial advantage
  - Unauthorised access to company’s system
- Misuse of the location of individual data

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Must be avoided or reduced</th>
<th>Absolutely avoided or reduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Significant</td>
<td></td>
<td>These risks may be taken</td>
<td>Must be reduced</td>
</tr>
<tr>
<td>Limited</td>
<td></td>
<td>Negligible Likelihood</td>
<td>Limited Likelihood</td>
</tr>
<tr>
<td>Negligible</td>
<td></td>
<td></td>
<td>Maximum Likelihood</td>
</tr>
</tbody>
</table>

Co-funded by the European Commission
Smart city use case session: Measures

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Use Case Measures

- Open data use case Incident management
  - Smart city PR, Smart city management team
  - Periodic incident drill
  - Remove open data repository

- Removing the data
- Maintain traceability of open data processing
- Information security (access)
- To have updated anonymization processes
- Transparency

- Bike sharing session
  - Fake data
    - Plausibility check
    - Anomaly detection
Smart city use case session: Conclusions

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018
Conclusion: ISO/IEC 27570 Privacy guidelines for smart cities

• Time line
  • February 2018 - Acceptance of project
  • May 2018 - 1st Working draft
  • February 2021 or earlier - Standard publication

• Current content
  • Privacy in smart cities
    • Actors
    • Use cases example
    • Challenges for privacy
    • Common threats and risks
  • Guidelines for ecosystem coordination
    • Organisation application of security and privacy processes
    • Ecosystem application of security and privacy processes
  • Guidelines for smart city processes
    • Governance
    • Requirements
    • Risk analysis
    • Life cycle
    • Citizen engagement
Thank You!

The CREATE-IoT project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 732929.

e-mail: antonio.kung@trialog.com