As the Internet of Things (IoT) technologies are becoming widespread in our lives, privacy issues are significantly raising to the surface. The aim of this research is to develop a personal assistant that is able to answer software engineers questions about privacy practices during the design phase. Thus, there is a demanding need to develop a method that assists software developers to understand and apply the Privacy by Design (PbD) practices into their systems. We used semantic web technologies to model the knowledge of PbD schemes, their intersections with Privacy Patterns, IoT system needs, and the Privacy Patterns that should be applied in these IoT systems. In this paper, we are introducing the PARROT ontology that combines these pieces of knowledge. To assemble the PARROT ontology’s requirements, we first associated many real-world IoT use cases with a set of well-known Privacy Patterns that should be applied by the software developers. Then, we gathered Competency Questions (CQs) about these IoT use cases from researchers and software developers throw a series of workshops we conducted, and we curated with 81 CQs to be modeled. We proved the validation of the PARROT ontology and evaluated it with the Common Pitfalls with the help of Protégé & HermiT Reasoner, Ontology Pitfall Scanner (OOPS!), and external experts. We demonstrated the use of the PARROT ontology by user based study and found that the PARROT ontology is able to answer up to 58% of software engineers’ questions.
1 Introduction

In this document, we present the technical report for the phases of building the PARROT ontology. We present the six use cases with their descriptions and Data Flow Diagrams (DFDs). Then we set out the Ontology Requirements Specification Document (ORSD) which lists the purpose, scope, non-functional requirements, and functional requirements (i.e., Competency Questions (CQs)) for building the PARROT ontology. Afterwards, we put on view a table of the analysis of the information needs for the PARROT ontology. Next, we disclose the PARROT ontology RDF file. In addition, we display the validation of the PARROT ontology via SPARQL queries. Moreover, we present the show evaluation form that we made to assess the PARROT ontology. Finally, we reveal the content evaluation details that we collected from a user study. The full information about this information will be found in our published paper under the title: Quarriable Privacy by Design Knowledge Towards Augmenting Internet of Things Developer Capabilities and Knowledge.
2 Use Cases

• **Health Care System**
  Diabetes treatment and monitoring is an IoT application that analyses patient health data to issue alerts and notifications. The researcher needs to gather and analyze data from a Continuous Glucose Monitor (CGM) sensor device worn by her patients. The sensor measures glucose levels by taking readings at consistent intervals across several days. The researcher uses an application that can detect any triggers for blood glucose levels. This application analyses the gathered data and produces a notification to both the patient and the nurse. In addition to the researcher, the nurse, and the doctor have access to patient data for follow-up purposes. The figure 1 shows the DFD of the system.

• **Fitness Watch**
  Fitness Watch is a system that keeps records of data subjects’ activities. It also sends the data to the cloud and allows the data subject to access them via an online website. The figure 2 shows the DFD of the system.
Real Tracking Location System (RTLS) aims to help the driver to find where he parked his car. It is considered as a real-time tracking solution where it stores and retrieves the parked car location in a centralized system. As the figure illustrates the use case, the location data will be sent by the GPS device embedded in the car via the gateway to be stored in the cloud. When the user wants to get this information, he requests the location data via a provided mobile application. Thus, the application will retrieve the car location and show it to the user. The figure 3 shows the DFD of the system.

Park Monitoring System is designed for a park theme that facilitates many rides for visitors with a waiting queue. This system will help to get expected waiting time for each ride. A snapshot for the queue will be taken from a camera device, the photos will be analysed by applying a specific API. Then, the analysed data will be sent from the park edge to the cloud environment via the gateway. The supervising team are able to monitor the status for each ride from the monitoring edge. They can request and retrieve the data from the cloud environment via the gateway. The figure 4 shows the DFD of the system.
• **Smart Home System**
  Smart home system has many sensors in the house that are connected to the cloud to either observe or control the devices in the home. The figure 5 shows the DFD of the system.

• **Drone Delivery System**
  Drone delivery is a system that makes shipments to customers’ homes. When the shipping company packs the shipment in a box of the drone, they use the GPS and the Camera to guide the drone to the right home. The figure 6 shows the DFD of the system.
3 Ontology Requirements Specification Document (ORSD)

1. **Purpose** The purpose of building the PARROT ontology is to combine the knowledge of privacy-preserving schemes and IoT devices for systematic guidance to software developers when designing IoT systems.

2. **Scope** The ontology will include the 10 Privacy by Design (PbD) schemes cited in the technical report, IoT knowledge. In addition, it encapsulates the associations of IoT and PbD schemes to answer the competency questions stated in this document.

3. **Implementation Language** The ontology must be implemented in the OWL2 language.

4. **Intended End-Users** User1. Software developers who are intending to apply privacy-preserving practices in the design phase of their systems. User2. Researchers who are looking for a modeled knowledge of privacy schemes and IoT sensors for different purposes.

5. **Intended Uses** Use1. For tools that need a semantic knowledge base to get information about applying privacy-preserving practices. Use2. For companies and organizations who intend to apply privacy-preserving practices.

6. **Ontology Requirements**
   
   (a) **Non-Functional Requirements**
   
   NFR1. The ontology must include all Privacy by Design (PbD) schemes stated in the technical report.
   
   NFR2. The ontology must include the relationship between the different PbD schemes as stated in the technical report.
   
   NFR3. The ontology must identify similar PbD schemes.
   
   NFR4. The ontology must include the IoT components.
   
   NFR5. The ontology must include the IoT components and their associated Privacy Patterns.

   (b) **Functional Requirements: Groups of Competency Questions**

   **CQG1. Health System (11 CQ)**
   
   CQ1. What are PbD patterns I should apply if my system includes a user interface/ mobile application/ screen/ mobile phone?
   
   CQ2. What are PbD patterns I should apply if my system stores data subject’s information in a cloud-based data base?
   
   CQ3. What are PbD patterns I should apply if my system reports data subject’s information to an Administrator/ Controller?
   
   CQ4. What are PbD patterns I should apply if my system shares data subject’s information to a third party/ another organization?
   
   CQ5. What are PbD patterns I should apply if my system requires collecting Personal Data?
   
   CQ6. What are PbD patterns I should apply if my system includes a Sensor/ device that collects data?
   
   CQ7. What are PbD patterns I should apply if my system routes data subject’s information among the system components/ nodes?
   
   CQ8. What are the PbD privacy patterns I should apply if my system requires user login?
   
   CQ9. What are the PbD privacy patterns I should apply to allow data subject to have control on his stored data?
   
   CQ10. What are the PbD privacy patterns I should apply to allow data subject to choose his collected data?
   
   CQ11. What are the PbD privacy patterns I should apply if my system collects data subject’s location?

   **CQG2. Drone Delivery (9 CQ)**
   
   CQ12. What are PbD patterns I should apply if my system provides tracking service?
   
   CQ13. What are PbD patterns I should apply if my system was attacked?
   
   CQ14. What are PbD patterns I should apply if my system stores address data that belong to previous customers?
   
   CQ15. What are PbD patterns I should apply if my system has the possibility of being infiltrated?
   
   CQ16. What are PbD patterns I should apply if my system allows customers to delete their data at any time?
   
   CQ17. What are PbD patterns I should apply if my system provides cloud access to customers as well?
CQ18. What are PbD patterns I should apply if my system provides drone access to more than one users (pilots) to provide required services?
CQ19. What are PbD patterns I should apply if my system requires 24 hour monitoring?
CQ20. What are PbD patterns I should apply if my system save historical data for how long?
CQ21. What are PbD patterns I should apply if my system recorded sensitive information about customers?

**CQG3. Fitness Watch (30 CQ)**
CQ22. What are PbD patterns I should apply to ensure data subject’s advantage?
CQ23. What are PbD patterns I should apply to ensure my system does not collect data more than what is stated in the privacy policy?
CQ24. What are the PbD patterns I should apply if the system capabilities such as microphone is always on?
CQ25. What are PbD patterns I should apply if my system shares data subject’s information with third party. e.g., insurance companies?
CQ26. What are the PbD patterns I should apply if my system allow trusted parties to access my data?
CQ27. What are the PbD patterns I should apply if the system is collecting/ gathers data subject’s information?
CQ28. What are PbD patterns I should apply to notify the data subject about his data collection?
CQ29. What are PbD patterns I should apply to allow data subject to control his data?
CQ30. What are PbD patterns I should apply if my system detects a criminal behaviour?
CQ31. What are PbD patterns I should apply if my system shares the the collected data between Data subjects?
CQ32. What are PbD patterns I should apply if my system stores data in the cloud?
CQ33. What are PbD patterns I should apply if my system store data in the smart watch?
CQ34. What are PbD patterns I should apply if my system keeps user’s real-time location in cloud
CQ35. What are PbD patterns I should apply if my system store the location in the cloud?
CQ36. What are PbD patterns I should apply if my system can store the data in the mobile?
CQ37. What are PbD patterns I should apply if my system keeps the data for a period of time?
CQ38. What are PbD patterns I should apply if my system sell the users info with third parties?
CQ39. What are PbD patterns I should apply if my system collects user’s age, gender, marital status and other personal information is required?
CQ40. What are PbD patterns I should apply if my system stores user’s food intake information?
CQ41. What are PbD patterns I should apply if my system stores user’s gym information?
CQ42. What are PbD patterns I should apply if I do not need the identity of the user? (anonymise)
CQ43. What are PbD patterns I should apply to prevent attackers from identify the identity of the user?
CQ44. What are PbD patterns I should apply if my system requires user’s city information?
CQ45. What are PbD patterns I should apply to allow the user to delete his data if he/she wants to do?
CQ46. What are PbD patterns I should apply if my system requires user’s address?
CQ47. What are PbD patterns I should apply to give user privacy notification in case he/she wants to share personal data e.g exact location?
CQ48. What are PbD patterns I should apply if my system scans wireless access points for indoor positioning?
CQ49. What are PbD patterns I should apply if my system have attack/threats?
CQ50. What are PbD patterns I should apply if my system stores user’s daily routine?
CQ51. What are PbD patterns I should apply if my system requires user’s device’s properties?
CQ52. What are PbD patterns I should apply if my system shares user’s accident information to emergency services?

**CQG4. Park Monitoring (9 CQ)**
CQ53. What are PbD patterns I should apply if my system store people faces/ photos (identifiable info)?
CQ54. What are PbD patterns I should apply if my system allows administration staff to view the images?
CQ55. What are PbD patterns I should apply to make sure non authorised people (staff) accessing
the images?
CQ56. What are PbD patterns I should apply if my system send raw data ex: people faces?
CQ57. What are PbD patterns I should apply if my system detect age, gender or other properties of
customers?
CQ58. What are PbD patterns I should apply to make my system analyse (aggregation) the data in
the cloud?
CQ59. What are PbD patterns I should apply to make sure the data subject has the right to delete
his data?
CQ60. What are PbD patterns I should apply if my system save the videos for long time?
CQ61. What are PbD patterns I should apply if my system allows real-time monitoring of the
images locally?

**CQG5. Real-Time Tracking System RTLS (10 CQ)**

CQ62. What are PbD patterns I should apply if my system is storing the data in the cloud?
CQ63. What are PbD patterns I should apply if my system is sharing data subject’s information
with third party?
CQ64. What are PbD patterns I should apply if my system is being used in different countries
applying different privacy policies?
CQ65. What are PbD patterns I should apply if my system is notifying the users?
CQ66. What are PbD patterns I should apply if my system is collecting the data continuously?
CQ67. What are PbD patterns I should apply if my system is sending subject’s data to the server?
CQ68. What are PbD patterns I should apply if my system is processing subject’s data?
CQ69. What are PbD patterns I should apply if GPS tracking the car?
CQ70. What are PbD patterns I should apply if my system requires contacting the data subject e.g.,
by phone, email, etc.?
CQ71. What are PbD patterns I should apply if my system can be paired with other IoT devices?

**CQG6. Smart Home (10 CQ)**

CQ72. What are PbD patterns I should apply if the TV preferred shows and episodes be shared and
accessed by third parties?
CQ73. What are PbD patterns I should apply if my system allows data subject to choose which
data and how much data to be shared across connected devices?
CQ74. What are PbD patterns I should apply if my system connects multiple smart devices and
synced data across them?
CQ75. What are PbD patterns I should apply if my system has the possibility of being infiltrated?
CQ76. What are PbD patterns I should apply if my system stores clients’ data in a secure manner?
CQ77. What are PbD patterns I should apply if my system records audio when I have a private talk
with my home mates?
CQ78. What are PbD patterns I should apply if my system requests a consent from data subject to
store his data?
CQ79. How do you deal with outdoor cameras if they record strangers?
CQ80. What are PbD patterns I should apply if my system suspects intruder or privacy invasion?
CQ81. What are PbD patterns I should apply if my system has cameras?

## 4 Data Set

<table>
<thead>
<tr>
<th>CQ</th>
<th>Type</th>
<th>Sub-type</th>
<th>Rank</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minimize</td>
<td>Hike</td>
<td>Separate</td>
<td>Aggregate</td>
</tr>
<tr>
<td>Health System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8
| 6 | What are PbD patterns I should apply if my system includes a sensor/device that collects data? | Device | Sensor | Valid | 19. Ambiguous Notice | 4. Informed Secure Passwords | 71. Unusual Activities | X |
| 7 | What are PbD patterns I should apply if my system routes data subject’s information among the system components/nodes? | Process | Route | Valid | 24. Onion Routing | 29. Aggregation Gateway | X X X |
| 8 | What are the PbD privacy patterns I should apply if my system requires user login? | Process | Profile | Valid | 4. Informed Secure Passwords | 71. Unusual Activities | X |
| 9 | What are the PbD privacy patterns I should apply to allow data subject to have control on his stored data? | Regulations | Control | Duplicated | 35. Enable/Disable Function | 45. Platform for Privacy Preferences | 54. Reasonable Level of Control | X X |
| 10 | What are the PbD privacy patterns I should apply to allow data subject to choose his collected data? | Regulations | Control | Valid | 35. Enable/Disable Function | 45. Platform for Privacy Preferences | 54. Reasonable Level of Control | X X |
| 11 | What are the PbD privacy patterns I should apply if my system collects data subject’s location? | Data Collection | Location | Valid | 2. Location Granularity | X X |

**Drone Delivery**

<p>| 13 | was attacked? | Regulations | Notify | Modified Duplicated | 22. Data Breach Notification Pattern | 71. Unusual Activities | X |
| 14 | stores address data that belong to previous customers? | Regulations Agreement | Duplicated | 50. Obligation Management | X X |
| 15 | has the possibility of being infiltrated? | Regulations | Notify | Duplicated | 71. Unusual Activities | X |
| 16 | allows customers to delete their data at any time? | Regulations | Control | Duplicated | 48. Privacy Dashboard | 61. Personal Data Table | X X X |
| 17 | provides cloud access to customers as well? | Process | Access | Valid | 27. Personal Data Store | 48. Privacy Dashboard | 61. Personal Data Table | X X X |
| 18 | provides drone access to more than one users (pilots) to provide required services? | Process | Access | Valid | 5. Awareness Feed | 9. Who’s Listening | 9. Who’s Listening | X X |
| 20 | save historical data for how long? | Regulations Agreement | Duplicated | 3. Awareness Feed | 42. Appropriate Privacy Feedback | 50. Obligation Management | 57. Privacy Awareness Panel | X X X |</p>
<table>
<thead>
<tr>
<th>21</th>
<th>recorded sensitive information about customers?</th>
<th>Data Collection</th>
<th>Personal Information</th>
<th>Valid</th>
<th>8. Use of dummies</th>
<th>32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context</th>
<th>63. Added-noise measurement obfuscation</th>
<th>X</th>
<th>X</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fitness Watch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>What are PbD patterns I should apply to ensure data subject’s advantage?</td>
<td>Regulations Advantage</td>
<td>Valid</td>
<td>13. Reciprocity</td>
<td>17. Incentivized Participation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>What are PbD patterns I should apply to ensure my system does not collect data more than what is stated in the privacy policy?</td>
<td>Regulations Agreement</td>
<td>Modified</td>
<td>28. Trust Evaluation of Services Slides</td>
<td>32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>What are the PbD patterns I should apply if the system capabilities such as microphone is always on?</td>
<td>Device</td>
<td>Microphone</td>
<td>Valid</td>
<td>14. Asynchronous notice</td>
<td>19. Ambient Notice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>What are PbD patterns I should apply if my system shares data subject’s information with third party, e.g., insurance companies?</td>
<td>Process</td>
<td>Third Party</td>
<td>Duplicated</td>
<td>18. Outsourcing [with consent]</td>
<td>50. Obligation Management</td>
<td>60. Sticky Policies</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>What are PbD patterns I should apply to notify the data subject about his data collection?</td>
<td>Regulations Notify</td>
<td>Valid</td>
<td>5. Awareness Feed</td>
<td>14. Asynchronous notice</td>
<td>19. Ambient Notice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>What are PbD patterns I should apply to allow data subject to control his data?</td>
<td>Regulations Control</td>
<td>Duplicated</td>
<td>27. Personal Data Store</td>
<td>35. Enable/Disable Function</td>
<td>45. Platform for Privacy Preferences</td>
<td>48. Privacy Dashboard</td>
<td>54. Reasonable Level of Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>What are PbD patterns I should apply if my system stores data in the cloud</td>
<td>Storage</td>
<td>Cloud</td>
<td>Duplicated</td>
<td>2. Location Granularity</td>
<td>8. Use of dummies</td>
<td>44. Decoupling [content] and Location Information Visibility</td>
<td>63. Added-noise measurement obfuscation</td>
<td>64. Increasing Awareness of Information Aggregation</td>
<td>74. Dynamic Location Granularity</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>What are PbD patterns I should apply if my system store data in the smart watch?</td>
<td>Storage</td>
<td>Local</td>
<td>Modified Duplicated</td>
<td>27. Personal Data Store</td>
<td>38. User Data Confinement Pattern</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>What are PbD patterns I should apply if my system keeps user’s real-time location in cloud</td>
<td>Data Collection</td>
<td>Location</td>
<td>Valid</td>
<td>3. Awareness Feed</td>
<td>35. Enable/Disable Function</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>What are PbD patterns I should apply if my system store the location in the cloud?</td>
<td>Storage</td>
<td>Cloud</td>
<td>Valid</td>
<td>2. Location Granularity</td>
<td>44. Decoupling [content] and Location Information Visibility</td>
<td>63. Added-noise measurement obfuscation</td>
<td>64. Increasing Awareness of Information Aggregation</td>
<td>74. Dynamic Location Granularity</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>36</td>
<td>What are PbD patterns I should apply if my system can store the data in the mobile?</td>
<td>Storage</td>
<td>Local</td>
<td>Modified Duplicated</td>
<td>27. Personal Data Store</td>
<td>38. User Data Confinement Pattern</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>What are PbD patterns I should apply if my system keeps the data for a period of time</td>
<td>Regulations Agreement</td>
<td>Modified Duplicated</td>
<td>32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context</td>
<td>40. Obtaining Explicit Consent</td>
<td>58. Legal Consent</td>
<td>59. Privacy Aware Wording</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>44</td>
<td>What are PbD patterns I should apply if my system requires user’s city information</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Valid</td>
<td>2. Location Granularity</td>
<td>29. Aggregation Gateway</td>
<td>38. User Data Confinement Pattern</td>
<td>41. Privacy Mirrors</td>
<td>48. Privacy Dashboard</td>
<td>61. Personal Data Table</td>
<td>64. Increasing Awareness of Information Aggregation</td>
</tr>
<tr>
<td>45</td>
<td>What are PbD patterns I should apply to allow the user to delete his data if he/she wants to do?</td>
<td>Regulations Control</td>
<td>Duplicated</td>
<td>28. Privacy Dashboard</td>
<td>61. Personal Data Table</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>What are PbD patterns I should apply if my system requires user’s address</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Valid</td>
<td>2. Location Granularity</td>
<td>29. Aggregation Gateway</td>
<td>38. User Data Confinement Pattern</td>
<td>41. Privacy Mirrors</td>
<td>48. Privacy Dashboard</td>
<td>61. Personal Data Table</td>
<td>64. Increasing Awareness of Information Aggregation</td>
</tr>
<tr>
<td>47</td>
<td>What are PbD patterns I should apply to give user privacy notification in case he/she wants to share personal data e.g exact location ?</td>
<td>Process</td>
<td>Share</td>
<td>Valid</td>
<td>12. Discouraging Blanket Strategies</td>
<td>46. Selective Access control</td>
<td>55. Masquerade</td>
<td>56. Buddy List</td>
<td>67. [Support] Selective Disclosure</td>
<td>68. Private Link</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>What are PbD patterns I should apply if my system scans wireless access points for indoor positioning</td>
<td>Data Collection</td>
<td>Location</td>
<td>Valid</td>
<td>14. Asynchronous notice</td>
<td>19. Ambient Notice</td>
<td>35. Enable/Disable Function</td>
<td>42. Appropriate Privacy Feedback</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>What are PbD patterns I should apply if my system have attack/threats?</td>
<td>Regulations Notify</td>
<td>Duplicated</td>
<td>22. Data Breach Notification Pattern</td>
<td>71. Unusual Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>What are PbD patterns I should apply if my system stores user’s daily routine?</td>
<td>Data Collection</td>
<td>Route</td>
<td>Valid</td>
<td>50. Obligation Management</td>
<td>51. Informed Credential Selection</td>
<td>54. Reasonable Level of Control</td>
<td>57. Privacy Awareness Panel</td>
<td>61. Personal Data Table</td>
<td>63. Added-noise measurement obfuscation</td>
<td>64. Increasing Awareness of Information Aggregation</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------</td>
<td>-------</td>
<td>--------------------------</td>
<td>--------------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>51</td>
<td>What are PbD patterns I should apply if my system requires user’s device’s properties</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Valid</td>
<td>12. Discouraging Blanket Strategies</td>
<td>46. Selective Access control</td>
<td>55. Masquerade</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>What are PbD patterns I should apply if my system shares user’s accident information to emergency services</td>
<td>Process</td>
<td>Third Party</td>
<td>Valid</td>
<td>18. Outsourcing [with consent]</td>
<td>50. Obligation Management</td>
<td>60. Sticky Policies</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>What are PbD patterns I should apply if my system allows administration staff to view the images</td>
<td>Process</td>
<td>Access</td>
<td>Valid</td>
<td>40. Obtaining Explicit Consent</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>What are PbD patterns I should apply to make sure non authorised people (staff) accessing the images?</td>
<td>Regulations Agreement</td>
<td>Modified</td>
<td>28. Trust Evaluation of Services Slides</td>
<td>32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>What are PbD patterns I should apply if my system send raw data ex: people faces?</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Valid</td>
<td>35. User Data Confinement Pattern</td>
<td>65. Attribute Based Credentials</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>What are PbD patterns I should apply if my system detect age, gender or other properties of customers</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Valid</td>
<td>3. Minimal Information Asymmetry</td>
<td>40. Obtaining Explicit Consent</td>
<td>59. Privacy Aware Wording</td>
<td>65. Attribute Based Credentials</td>
<td>69. Anonymity Set</td>
<td>X X X X X X</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>What are PbD patterns I should apply if my system analyse the data in the cloud? (aggregation)</td>
<td>Process</td>
<td>Route</td>
<td>Modified</td>
<td>65. Attribute Based Credentials</td>
<td>69. Anonymity Set</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>What are PbD patterns I should apply to make sure the data subject has the right to delete his data?</td>
<td>Regulations Agreement</td>
<td>Duplicated</td>
<td>28. Trust Evaluation of Services Slides</td>
<td>32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>What are PbD patterns I should apply if my system save the videos for long time?</td>
<td>Regulations Agreement</td>
<td>Duplicated</td>
<td>3. Minimal Information Asymmetry</td>
<td>59. Privacy Aware Wording</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Park Monitoring**

| #  | What are PbD patterns I should apply if my system is processing subject’s data? | Data Collection | Routine | Valid | 15. Outsourcing [with consent] | 50. Obligation Management | 60. Sticky Policies | X |
|----|--------------------------------------------------------------------------------|----------------|-------|-------|--------------------------|--------------------------------|-------------------------------|-----------------------------------------------|-----------------------------------------------|
| 64 | What are PbD patterns I should apply if my system is being used in different countries applying different privacy policies? | Regulations Privacy Policy | Valid | X X X X |
| 65 | What are PbD patterns I should apply if my system is notifying the users? | Regulations Notify | Valid | 14. Asynchronous notice | 19. Ambient Notice | X |
| 66 | What are PbD patterns I should apply if my system is collecting the data continuously? | Data Collection | Routine | Valid | 14. Asynchronous notice | 19. Ambient Notice | 42. Appropriate Privacy Feedback | 70. Active Broadcast of Presence | X X X |
| 67 | What are PbD patterns I should apply if my system is sending subject’s data to the server? | Process | Route | Valid | 24. Onion Routing | 43. Impactful Information and Feedback | X X X |
| 68 | What are PbD patterns I should apply if my system is processing subject’s data? | Process | Route | Valid | 28. Trust Evaluation of Services Slides | 38. User Data Confinement Pattern | X X X X |
| --- | --- | --- |
| CQ2. | What are PbD patterns I should apply if my system stores data subject’s information in a cloud-based data base? | SELECT ?DataActivity ?PrivacyPattern WHERE ?DataActivity a gdprtext:DataActivity. ?DataActivity parrot:entails ?PrivacyPattern. FILTER (?DataActivity = parrot:Store_Data) |
CQ4. What are PbD patterns I should apply if my system shares data subject’s information to a third party/another organization?

```
SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Share_Personal_Data_with_Third_Party)
```

CQ5. What are PbD patterns I should apply if my system requires collecting Personal Data?

```
SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Collection_of_Personal_Data)
```

CQ6. What are PbD patterns I should apply if my system includes a Sensor/device that collects data?

```
SELECT ?Sensor ?PrivacyPattern
FILTER (?Sensor = parrot:Glucose_Sensor)
```

CQ7. What are PbD patterns I should apply if my system routes data subject’s information among the system components/nodes?

```
SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Route_Data)
```

CQ8. What are the PbD privacy patterns I should apply if my system requires user login?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:IdentificationOfDataSubject.
FILTER (?Activity = parrot:Login)
```

CQ9. What are the PbD privacy patterns I should apply to allow data subject to have control on his stored data?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ExerciseRights.
FILTER (?Activity = parrot:Data_subject_controls_his_data)
```

CQ10. What are the PbD privacy patterns I should apply to allow data subject to choose his collected data?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ExerciseRights.
FILTER (?Activity = parrot:Data_subject_chooses_collected_data)
```

CQ11. What are the PbD privacy patterns I should apply if my system collects data subject’s location?

```
SELECT ?Data ?PrivacyPattern
WHERE ?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Location)
```

CQ12. What are PbD patterns I should apply if my system provides tracking service?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Tracking)
```

CQ13. What are PbD patterns I should apply if my system was attacked?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Notification_Activity.
FILTER (?Activity = parrot:Notify_System_Attack)
```

CQ14. What are PbD patterns I should apply if my system stores address data that belong to previous customers?

```
```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ArchiveData.
FILTER (?Activity = parrot:Historical_Data)

CQ15. What are PbD patterns I should apply if my system has the possibility of being infiltrated?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Notification_Activity.
FILTER (?Activity = parrot:Notify_Data_Infiltration)

CQ17. What are PbD patterns I should apply if my system allows customers to delete their data at any time?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:DataActivity.
FILTER (?Activity = parrot:Delete_Data)

CQ19. What are PbD patterns I should apply if my system provides drone access to more than one users (pilots) to provide required services?

SELECT ?Activity ?PrivacyPattern
FILTER (?Activity = parrot:to_service_provider)

CQ20. What are PbD patterns I should apply if my system requires 24 hour monitoring?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:24_Hour_Monitoring)

CQ21. What are PbD patterns I should apply if my system save historical data for how long?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ArchiveData.
FILTER (?Activity = parrot:Historical_Data)

CQ22. What are PbD patterns I should apply if my system recorded sensitive information about customers?

SELECT ?Data ?PrivacyPattern
WHERE ?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Sensitive_personal_information)

Fitness Watch

CQ23. What are PbD patterns I should apply to ensure data subject’s advantage?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ExerciseRights.
FILTER (?Activity = parrot:Ensure_data_subjects_advantage)

CQ24. What are PbD patterns I should apply to ensure my system does not collect data more than what is stated in the privacy policy?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ObligationForCollectionOfPersonalData.
FILTER (?Activity = parrot:Specified_in_the_privacy_policy)

CQ25. What are the PbD patterns I should apply if the system capabilities such as microphone is always on?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Device_Always_On)
CQ25. What are PbD patterns I should apply if my system shares data subject’s information with third party. e.g., insurance companies?

```
SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Share_Personal_Data_with_Third_Party)
```

CQ26. What are the PbD patterns I should apply if my system allow trusted parties to access my data?

```
SELECT ?Activity ?PrivacyPattern
FILTER (?Activity = parrot:to_trusted_parties )
```

CQ27. What are the PbD patterns I should apply if the system is collecting/ gathers data subject’s information?

```
SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Collection_of_Personal_Data)
```

CQ28. What are PbD patterns I should apply to notify the data subject about his data collection?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Notification_Activity.
FILTER (?Activity = parrot:Notify_Data_Collection)
```

CQ29. What are PbD patterns I should apply to allow data subject to control his data?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ExerciseRights.
FILTER (?Activity = parrot:Data_subject_controls_his_data)
```

CQ30. What are PbD patterns I should apply if my system detects a criminal behaviour?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Notification_Activity.
FILTER (?Activity = parrot:Notify_System_Attack)
```

CQ31. What are PbD patterns I should apply if my system shares the the collected data between Data subjects?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Share_Data.
FILTER (?Activity = parrot:to_another_user)
```

CQ32. What are PbD patterns I should apply if my system stores data in the cloud?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:StoreData.
FILTER (?Activity = parrot:in_cloud)
```

CQ33. What are PbD patterns I should apply if my system store data in the smart watch?

```
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:StoreData.
FILTER (?Activity = parrot:Locally)
```

CQ34. What are PbD patterns I should apply if my system keeps user’s real-time location in cloud?

```
SELECT ?Data ?PrivacyPattern
WHERE ?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Real_Time_Location)
```

CQ35. What are PbD patterns I should apply if my system store the location in the cloud?

```
CQ36. What are PbD patterns I should apply if my system can store the data in the mobile?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:StoreData.
FILTER (?Activity = parrot:Store_Location)

CQ37. What are PbD patterns I should apply if my system keeps the data for a period of time?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:StoreData.
FILTER (?Activity = parrot:Locally)

CQ38. What are PbD patterns I should apply if my system sell the users info with third parties?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Share_Data.
FILTER (?Activity = parrot:sell_data)

CQ39. What are PbD patterns I should apply if my system collects user’s age, gender, marital status and other personal information is required?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Collecting_Personal_Information)

CQ40. What are PbD patterns I should apply if my system stores user’s food intake information?

SELECT ?Data ?PrivacyPattern
WHERE ?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Food_Data)

CQ41. What are PbD patterns I should apply if my system stores user’s gym information?

SELECT ?Data ?PrivacyPattern
WHERE ?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Gym_Data)

CQ42. What are PbD patterns I should apply if I do not need the identity of the user? (anonymously)

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Anonymously)

CQ43. What are PbD patterns I should apply to prevent attackers from identify the identity of the user?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ExerciseRights.
FILTER (?Activity = parrot:Hide_data_subjects_identity_from_attackers)

CQ44. What are PbD patterns I should apply if my system requires user’s city information?

SELECT ?Data ?PrivacyPattern
WHERE ?Personal_Data rdf:type gdprtext:PersonalData.
filter (?Data = parrot:City)

CQ45. What are PbD patterns I should apply to allow the user to delete his data if he/she wants to do?
CQ46. What are PbD patterns I should apply if my system requires user’s address?

```
SELECT ?Personal_Data ?PrivacyPattern
WHERE
?Personal_Data rdf:type gdprtext:PersonalData.
FILTER ( ?Personal_Data = parrot:Address )
```

CQ47. What are PbD patterns I should apply to give user privacy notification in case he/she wants to share personal data exact location?

```
SELECT ?Activity ?PrivacyPattern
WHERE
?Activity a parrot:Share_Data.
FILTER ( ?Activity = parrot:user_to_user )
```

CQ48. What are PbD patterns I should apply if my system scans wireless access points for indoor positioning?

```
SELECT ?Data ?PrivacyPattern
WHERE
?Data a gdprtext:PersonalData.
FILTER ( ?Data = parrot:Indoor_positioning )
```

CQ49. What are PbD patterns I should apply if my system have attack/threats?

```
SELECT ?Activity ?PrivacyPattern
WHERE
?Activity a parrot:Notification_Activity.
FILTER (?Activity = parrot:Notify_System_Attack)
```

CQ50. What are PbD patterns I should apply if my system stores user’s daily routine?

```
SELECT ?Data ?PrivacyPattern
WHERE
?Data a gdprtext:PersonalData.
FILTER ( ?Data = parrot:Daily_Routine )
```

CQ51. What are PbD patterns I should apply if my system requires user’s device’s properties?

```
SELECT ?Data ?PrivacyPattern
WHERE
?Data a gdprtext:PersonalData.
FILTER ( ?Data = parrot:Data_subjects_device_properties )
```

CQ52. What are PbD patterns I should apply if my system shares user’s accident information to emergency services?

```
SELECT ?Activity ?PrivacyPattern
WHERE
?Activity a parrot:Share_Data.
FILTER ( ?Activity = parrot:to_emergency_services )
```

```
Park Monitoring System
```

CQ53. What are PbD patterns I should apply if my system store people faces/ photos ( identifiable info)?

```
SELECT ?Data ?PrivacyPattern
WHERE
?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Face_photo)
```

CQ54. What are PbD patterns I should apply if my system allows administration staff to view the images?

```
SELECT ?Activity ?PrivacyPattern
WHERE
FILTER (?Activity = parrot:to_administrator )
```

CQ55. What are PbD patterns I should apply to make sure non authorised people (staff) accessing the images?
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:Compliance.
FILTER (?Activity = parrot:Non-authorized_people_access)

CQ56. What are PbD patterns I should apply if my system send raw data ex: people faces?

SELECT ?Data ?PrivacyPattern
WHERE ?Data a gdprtext:PersonalData.
FILTER (?Data = parrot:Raw_Data)

CQ57. What are PbD patterns I should apply if my system detect age, gender or other properties of customers

SELECT ?Personal_Data ?PrivacyPattern
WHERE ?Personal_Data rdf:type gdprtext:PersonalData.
filter (?Personal_Data = parrot:Age)

SELECT ?Personal_Data ?PrivacyPattern
WHERE ?Personal_Data rdf:type gdprtext:PersonalData.
filter (?Personal_Data = parrot:Gender)

CQ58. What are PbD patterns I should apply to make my system analyse the data in the cloud? (aggregation)

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Route_Data.
FILTER (?Activity = parrot:to_cloud)

CQ59. What are PbD patterns I should apply to make sure the data subject has the right to delete his data?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:ExerciseRights.
FILTER (?Activity = parrot:Data_subject_deletes_his_data)

CQ60. What are PbD patterns I should apply if my system save the videos for long time?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:StoreData.
FILTER (?Activity = parrot:for_a_period_of_time)

CQ61. What are PbD patterns I should apply if my system allows real-time monitoring of the images locally?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Live_Video_Monitoring)

Real-Time Tracking System RTLS

CQ62. What are PbD patterns I should apply if my system is storing the data in the cloud?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:StoreData.
FILTER (?Activity = parrot:in_cloud)

CQ63. What are PbD patterns I should apply if my system is sharing data subject’s information with third party?

SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Share_Personal_Data_with_Third_Party)

CQ64. What are PbD patterns I should apply if my system is being used in different countries applying different privacy policies?
SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CrossBorderTransfer.
FILTER (?Activity = parrot:Used_in_Different_Countries)

CQ65. What are PbD patterns I should apply if my system is notifying the users?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Notification_Activity.
FILTER (?Activity = parrot:Notify_Users)

CQ66. What are PbD patterns I should apply if my system is collecting the data continuously?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Continuous_Data_Collection)

CQ67. What are PbD patterns I should apply if my system is sending subject’s data to the server?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Route_Data.
FILTER (?Activity = parrot:to_server)

CQ68. What are PbD patterns I should apply if my system is processing subject’s data?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:DataActivity.
FILTER (?Activity = parrot:Processing_Data)

CQ69. What are PbD patterns I should apply if GPS tracking the car?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:CollectionOfPersonalData.
FILTER (?Activity = parrot:Tracking)

CQ70. What are PbD patterns I should apply if my system requires contacting the data subject e.g., by phone, email, etc.?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:PersonalData.
FILTER (?Activity = parrot:Email || ?Activity = parrot:Phone)

CQ71. What are PbD patterns I should apply if my system can be paired with other IoT devices?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a parrot:Route_Data.
FILTER (?Activity = parrot:Between_Devices)

Smart Home System

CQ72. What are PbD patterns I should apply if the TV preferred shows and episodes be shared and accessed by third parties?

SELECT ?DataActivity ?PrivacyPattern
WHERE ?DataActivity a gdprtext:DataActivity.
FILTER (?DataActivity = parrot:Share_Personal_Data_with_Third_Party)

CQ73. What are PbD patterns I should apply if my system allows data subject to choose which data and how much data to be shared across connected devices?

SELECT ?Activity ?PrivacyPattern
WHERE ?Activity a gdprtext:DataActivity.
FILTER (?Activity = parrot:Choose_Data)

CQ74. What are PbD patterns I should apply if my system connects multiple smart devices and synced data across them?
Table 2: The PARROT ontology validation via SPARQL queries. The table shows the CQs grouped regarding the use cases and their SPARQL queries.
6 Evaluating the Common Pitfalls

6.1 Structural Dimension

<table>
<thead>
<tr>
<th>Pitfall</th>
<th>Element</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>P07. Merging different concepts in the same class.</td>
<td>Principles_of_Wright_and_Raab, Principles_of_Cavoukian_and_Jonas, Goals_of_Rost_and_Bock</td>
<td>The scanner considers these classes to have more than one concept because of the word “and”; however, these names refer to the same PhD scheme.</td>
</tr>
<tr>
<td>P13. Inverse relationships are not explicitly declared.</td>
<td>partially_inspired_by_fully_inspired_by_entails</td>
<td>In the PARROT ontology, we did not create an inverse relationship.</td>
</tr>
<tr>
<td>P19. Defining multiple domains or ranges in properties.</td>
<td>partially_inspired_by_fully_inspired_by_entails</td>
<td>We addressed this problem by typing the domains and ranges in the “Class expression editor” as a union of an intersection of multiple classes as a single domain/range.</td>
</tr>
</tbody>
</table>

Table 3: Structural Dimension Table. The table shows the pitfalls occurred in the OOPS! scanner and how they were assisted.

6.2 Functional Dimension

<table>
<thead>
<tr>
<th>Pitfall</th>
<th>Element</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>P10. Missing disjointness</td>
<td>This pitfall applies to the ontology in general instead of specific elements.</td>
<td>We declared some subclasses of GDPR:EXT:Principle and the sub-classes of parrot:Guideline as disjoint classes.</td>
</tr>
<tr>
<td>P08. Missing annotations.</td>
<td>PARROT:Sensor, PARROT:Goal, PARROT:Device, PARROT:Strategy</td>
<td>We added annotations to the ontology elements.</td>
</tr>
<tr>
<td>P13. Inverse relationships not explicitly declared.</td>
<td>partially_inspired_by_fully_inspired_by_entails</td>
<td>This pitfall was addressed in the first dimension.</td>
</tr>
<tr>
<td>P22. Using different naming conventions in the ontology</td>
<td>This pitfall applies to the ontology in general instead of specific elements.</td>
<td>Because we reused many ontologies, the naming conventions will vary. In the PARROT ontology we use an underscore between the words and capitalize the main words (for example: “parrot: Principles_of_Cavoukian”).</td>
</tr>
<tr>
<td>P41. No license declared.</td>
<td>The ontology metadata omits information about the license that applies to the ontology.</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Functional Dimension Table. The table shows the pitfalls occurred in the OOPS! scanner and how they were assisted.

6.3 Functional Dimension
Elements in PARROT | Annotation
---|---
1. PARROT:Sensor | An equivalent class to sosa:Sensor
2. PARROT:Privacy_by_Design_Schemes | A set of Privacy by Design goals created by different parties.
3. PARROT:Goal | A set of Privacy by Design guidelines created by different parties.
4. PARROT:Device | The devices used in the system.
5. PARROT:Strategy | A set of Privacy by Design strategies created by different parties.
6. PARROT:entails | The relationship between system components or activities with the privacy patterns.
7. PARROT:Privacy_Pattern | A set of Privacy by Design privacy patterns created by different parties. This level of Privacy by Design Schemes is linked to all the elements in other Privacy by Design Schemes. It is also linked to systems’ components and activities.
8. PARROT:Notification_Activity | The activity of notifying the data subject about any activity.
9. PARROT:Access_Data | The activity of providing access to the data for an individual or an organization. Ex: administrator.
10. PARROT:Share_Data | The activity of sharing some data subject’s information to an individual, a friend or an organization.
11. PARROT:Route_Data | The activity of routing data among different nodes of the system.

Table 6: The table shows PARROT elements and the annotation added to them

7 Expert Evaluation Form
### Parrot Ontology Expert Evaluation

**Contents**

- Introduction .................................................................................................................. 2  
  - General Description .................................................................................................... 2  
  - Evaluation Purpose .................................................................................................... 2  
  - Privacy and Confidentiality Statement ...................................................................... 2  
- Instructions .................................................................................................................. 3  
- Expert Participation .................................................................................................... 3  
- The Pitfalls To Examine ............................................................................................... 3  
- The PARROT Ontology ............................................................................................... 4  
- Reused Ontologies ..................................................................................................... 4  
  1. IoT Ontologies ........................................................................................................ 4  
  2. PbD Ontologies ........................................................................................................ 4  
- The PARROT Elements ............................................................................................... 5  
- Expert's Comments .................................................................................................... 8  
- References .................................................................................................................. 9
Introduction

General Description

The aim of the PARROT ontology (Privacy by Design for the Internet of Things) is to support a tool that will help software developers find the relevant Privacy by Design (PbD) Practices for their IoT systems. It models the different knowledge of PbD practices (we call them schemes) and their relationships. It also models IoT systems’ information and the PbD schemes required to be applied.

![PARROT ontology contained knowledge](image)

Evaluation Purpose

This evaluation aims at verifying whether the PARROT ontology in terms of its concepts and relationships suffers from several common pitfalls in ontologies. The list of the pitfalls we consider in this evaluation can be found in the next section, followed by the PARROT ontology structure.

Privacy and Confidentiality Statement

All responses, including any personal information, will be kept strictly confidential. Your data will only be used and accessed by the researchers working on this project.

For any problem do not hesitate to contact: Lamya Alkhariji (alkharijiLa@cardiff.ac.uk)
Expert Participation

You are kindly requested to carefully assess the PARROT ontology in terms of its concepts and relationships against several common pitfalls in ontologies. The pitfalls we consider in this evaluation are listed below, and the PARROT ontology can be found in the next section.

The Pitfalls to Examine

The pitfalls definitions in this document are retrieved from the online pitfalls catalog (https://oops.linkeddata.es/catalogue.jsp).

P01. Creating polysemous elements: An ontology element (class, object property, or datatype property) whose identifier has different senses is included in the ontology to represent more than one conceptual idea or property.

P02. Creating synonyms as classes: Several classes whose identifiers are synonyms are created and defined as equivalent (owl:equivalentClass) in the same namespace.

P07. Merging different concepts in the same class: A class whose name refers to two or more different concepts is created.

P09. Missing domain information: Part of the information needed for modeling the intended domain is not included in the ontology. This pitfall may be related to (a) the requirements included in the Ontology Requirement Specification Document (ORSD) that are not covered by the ontology, or (b) to the lack of knowledge that can be added to the ontology to make it more complete. In this project, we created our ORSD file which is available in a separate file (ORSD.pdf).

P17. Overspecializing a hierarchy: The hierarchy in the ontology is specialized in such a way that the final leaves are defined as classes and these classes will not have instances.

P21. Using a miscellaneous class: This pitfall refers to the creation of a class with the only goal of classifying the instances that do not belong to any of its sibling classes (classes with which the miscellaneous problematic class shares a common direct ancestor).
In this section, we will describe the reused ontology to model the information needed in the PARROT ontology. Furthermore, we will detail the hierarchy of the PARROT ontology. Please find the PARROT ontology file in the sent documents (PARROT.owl).

### Reused Ontologies

1. **IoT Ontologies**

   PARROT aims to help apply privacy patterns to IoT systems, thus, we needed to include IoT knowledge (i.e., devices and specifications) in our ontology. We used Semantic Sensor Network (SSN) ontology and its lightweight ontology SOSA (Sensor, Observation, Sample, and Actuator). They both describe sensors, actuators, samplers as well as their observations, actuation, and sampling activities [1]

   From SSN we used the class ssn:System and its subclasses such as sosa:Sensor to model the instances of IoT devices in our data set such as the instance 'Glucose Sensor'.

2. **PbD Ontologies**

   For PbD knowledge we found GDPRtEXT ontology that describes the concepts defined, mentioned and required by the General Data Protection Regulation (GDPR). GDPRtEXT uses the Simple Knowledge Organization System (SKOS) upper ontology which provides a model for expressing the basic structure and content of concept schemes. [2] [3]

   We used the class GDPRtEXT:Principle to include all PbD principles such as parrot:Principles_of_ISO_29100. We likewise used the class GDPRtEXT:PrivacybyDesign to include all PbD schemes classes such as parrot:Strategies_of_Hoepman and parrot:Privacy_Pattern. We also used other classes such as GDPRtEXT:Activity, GDPRtEXT:DataActivity. From SKOS ontology we used the class skos:Concept and many of its subclasses to model the knowledge of PbD. All used classes are detailed in PARROT elements section.
The PARROT Elements

Classes:

- skos:Concept
  - GDPRtEXT:Activity
    - GDPRtEXT:DataActivity
      - GDPRtEXT:ConsentActivity
        - GDPRtEXT:ObtainingConsent
      - PARROT:Access_Data
      - GDPRtEXT:ArchiveData
      - GDPRtEXT:CollectionOfPersonalData
      - GDPRtEXT:CrossBorderTransfer
      - PARROT:Route_Data
      - PARROT:Share_Data
      - GDPRtEXT:SharePersonalDataWithThirdParty
      - GDPRtEXT:StoreData
    - GDPRtEXT:ExerciseRights
    - GDPRtEXT:IdentificationOfDataSubject
    - PARROT:Notification_Activity
  - GDPRtEXT:Compliance
  - GDPRtEXT:Data
    - GDPRtEXT:PersonalData
  - PARROT:Privacy_by_Design_Schemes
    - GDPRtEXT:Principle
      - Parrot:Principles_of_Cavoukian
      - Parrot:Principles_of_FIPPs
      - Parrot:Principles_of_ISO_29100
      - Parrot:Principles_of_Wright_and_Raab
      - Parrot:Principles_of_Cavoukian_and_Jonas
    - Parrot:Strategy
      - Parrot:Strategies_of_Hoepman
    - Parrot:Goal
      - Parrot:Goals_of_Rost_and_Bock
    - Parrot:Guideline
      - Parrot:Guidelines_of_OECD
      - Parrot:Guidelines_of_Perera_et_al.
    - Parrot:Privacy_Pattern
- ssn:System
  - PARROT:Device
    - sosa:Sensor

Properties:

- parrot:fully_inspired_by
- parrot:partially_inspired_by
- parrot:entails

Figure 2 Class hierarchy of the PARROT ontology
<table>
<thead>
<tr>
<th>Element Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes</td>
</tr>
<tr>
<td>skos:Concept</td>
</tr>
<tr>
<td>GDPRtEXT:Activity</td>
</tr>
<tr>
<td>GDPRtEXT:DataActivity</td>
</tr>
<tr>
<td>GDPRtEXT:ConsentActivity</td>
</tr>
<tr>
<td>GDPRtEXT:ObtainingConsent</td>
</tr>
<tr>
<td>PARROT:Access_Data</td>
</tr>
<tr>
<td>GDPRtEXT:ArchiveData</td>
</tr>
<tr>
<td>GDPRtEXT:CollectionOfPersonalData</td>
</tr>
<tr>
<td>GDPRtEXT:CrossBorderTransfer</td>
</tr>
<tr>
<td>PARROT:Route_Data</td>
</tr>
<tr>
<td>PARROT:Share_Data</td>
</tr>
<tr>
<td>GDPRtEXT:SharePersonalDataWithThirdParty</td>
</tr>
<tr>
<td>GDPRtEXT:StoreData</td>
</tr>
<tr>
<td>GDPRtEXT:ExerciseRights</td>
</tr>
<tr>
<td>GDPRtEXT:IdentificationOfDataSubject</td>
</tr>
<tr>
<td>PARROT:Notification_Activity</td>
</tr>
<tr>
<td>GDPRtEXT:Compliance</td>
</tr>
<tr>
<td>GDPRtEXT:Data</td>
</tr>
<tr>
<td>GDPRtEXT:PersonalData</td>
</tr>
<tr>
<td>PARROT:Privacy_by_Design_Schemes</td>
</tr>
<tr>
<td>GDPRtEXT:Principle</td>
</tr>
<tr>
<td>PARROT:Strategy</td>
</tr>
<tr>
<td>PARROT:Goal</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>PARROT:Guideline</td>
</tr>
<tr>
<td>PARROT:Privacy_Pattern</td>
</tr>
<tr>
<td>ssn:System</td>
</tr>
<tr>
<td>PARROT:Device</td>
</tr>
<tr>
<td>sosa:Sensor</td>
</tr>
</tbody>
</table>

**Properties**

<p>| PARROT:entails               | The relationship between system components or activities with the privacy patterns. |
| PARROT:fully_inspired_by     | Is the relationship between the PbD schemes that indicates the connection between a privacy pattern and the other schemes (Principle, Guideline, and Strategy). This connection indicates a full inspiration for the privacy pattern from the privacy scheme. |
| PARROT:partially_inspired_by | Is the relationship between the PbD schemes that indicates the connection between a privacy pattern and the other schemes (Principle, Guideline, and Strategy). This connection indicates a partial inspiration for the privacy pattern from the privacy scheme. |</p>
<table>
<thead>
<tr>
<th>Pitfall</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References


### 8 Content Evaluation

<table>
<thead>
<tr>
<th>ID</th>
<th>Question</th>
<th>Rank</th>
<th>Type</th>
<th>Subtype</th>
<th>Use Case</th>
<th>SPARQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Will all data subject’s information will be sent to the cloud?</td>
<td>Discarded</td>
<td>Process</td>
<td>Access</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Report_for_Administration. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>If the system will send data subject’s information to the cloud, what can I do?</td>
<td>Valid</td>
<td>Process</td>
<td>Route</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Report_for_Administration. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>What protocols I can use to keep the data subject’s information safe during its routing to the cloud?</td>
<td>Valid</td>
<td>Process</td>
<td>Route</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Report_for_Administration. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>For how long I can keep the information in the cloud?</td>
<td>Valid</td>
<td>Regulation Agreement</td>
<td>Storage</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Share_Summary. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Can the data subject approve if all or some of his information will be shared?</td>
<td>Valid</td>
<td>Regulations</td>
<td>Control</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Will the data subject know exactly who can see his information?</td>
<td>Duplicated</td>
<td>Regulations</td>
<td>Control</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Do I need to inform the data subject about the people who will see his information?</td>
<td>Missing</td>
<td>Regulations</td>
<td>Privacy Policy</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>For how long I can keep the data subject’s information?</td>
<td>Duplicated</td>
<td>Regulations Agreement</td>
<td>Storage</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Will the doctor and the researcher have the data subject’s information associated with his personal information (i.e. name)? Or the information will be shared anonymously?</td>
<td>Valid</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Will the researcher and doctor have the same privilege? Will they have the same information?</td>
<td>Valid</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>What can we do to make the communication secure, from the sensor to the cloud and to the web application?</td>
<td>Valid</td>
<td>Process</td>
<td>Route</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Can we share a third party with the information as the researcher is?</td>
<td>Duplicated</td>
<td>Process</td>
<td>Third-Party</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>How can we guarantee the privacy of the information by the researcher?</td>
<td>Duplicated</td>
<td>Process</td>
<td>Third-Party</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>Do we need all the information that we asked from the data subject?</td>
<td>Duplicated</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
<tr>
<td>1</td>
<td>How do I store the information in the cloud? (ex: some methodology or protocols) to keep them safe?</td>
<td>Valid</td>
<td>Storage</td>
<td>Cloud</td>
<td>Health Care System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a parrot:Choose_Data. ?Activity parrot:entails 'PrivacyPattern. FILTER (?Activity = parrot:in_cloud) }</td>
</tr>
</tbody>
</table>
1 If we have an external copy or backup for the information, how can I keep them private?
Not available
Storage Cloud Health Care System

1 I need to send a report of the data subject to the doctor, how can I keep the data subject’s privacy?
Valid Process Share Health Care System

1 How can I keep the data subject’s information private inside the cloud?
Duplicated Storage Cloud Health Care System

1 What can I do if I send the information to the cloud (i.e. GPS data) continuously?
Valid Data Collection Routine Real Tracking Location System (RTLS)

1 Should the data subject turn on the functionality on and off?
Valid Regulations Control Real Tracking Location System (RTLS)

1 How can I make sure the data are sent to the cloud securely? (the communication)
Valid Process Route Real Tracking Location System (RTLS)

1 For how long I can keep the information in the cloud?
Valid Regulations Agreement Real Tracking Location System (RTLS)

1 Can have the identity of the data subject and have other information?
Valid Data Collection Personal Information Real Tracking Location System (RTLS)

1 If there was a third party, how can we deal with it?
Valid Process Third-Party Real Tracking Location System (RTLS)

1 Do the data subject have an idea about how this information will be stored or processed?
Missing Regulation Privacy Policy Real Tracking Location System (RTLS)

1 If the system got attacked and accessed the information what can we do?
Valid Regulations Notify Real Tracking Location System (RTLS)

1 Can we keep history of his information? Or shall they be deleted immediately?
Duplicated Regulation Agreement Real Tracking Location System (RTLS)
<table>
<thead>
<tr>
<th>1</th>
<th>Do someone else have access to this information other than the user?</th>
<th>Missing</th>
<th>Process</th>
<th>Access</th>
<th>Real Tracking Location System (RTLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Can we share the information with the authorities (ex: police) in case of a crime or emergency?</td>
<td>Valid</td>
<td>Process</td>
<td>Third-Party</td>
<td>Real Tracking Location System (RTLS)</td>
</tr>
<tr>
<td>1</td>
<td>Can we have non essential information (ex: car number, personal photo)?</td>
<td>Duplicated</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Real Tracking Location System (RTLS)</td>
</tr>
<tr>
<td>2</td>
<td>What information the nurses and doctors will get if the glucose sensor got abnormal readings?</td>
<td>Valid</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
</tr>
<tr>
<td>2</td>
<td>What kind of data the mobile app requires other than the name and age of the patient?</td>
<td>Discarded</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Health Care System</td>
</tr>
<tr>
<td>2</td>
<td>How to protect the data subject that are stored in the cloud?</td>
<td>Duplicated</td>
<td>Storage Cloud</td>
<td>Health Care System</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>How to protect the data subject’s privacy if more than one person is using the system?</td>
<td>Not available</td>
<td>Regulations Agreement</td>
<td>Health Care System</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>What are the research information the researchers have that will not violate the data subject’s privacy?</td>
<td>Valid</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
</tr>
<tr>
<td>2</td>
<td>Should the sensor be used by one person only or for more than one user (ex: husband and wife)?</td>
<td>Discarded</td>
<td>Health Care System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Who should have access to the CCTV cameras?</td>
<td>Missing</td>
<td>Process</td>
<td>Access</td>
<td>Smart Home System</td>
</tr>
<tr>
<td>2</td>
<td>Who should have access to the control tablets of the smart home?</td>
<td>Missing</td>
<td>Process</td>
<td>Access</td>
<td>Smart Home System</td>
</tr>
<tr>
<td>2</td>
<td>If something wrong happened (ex: thief in the house) people of the house should be informed.</td>
<td>Discarded</td>
<td>Notification</td>
<td>Smart Home System</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>If the parents of the kids don’t want them to watch TV?</td>
<td>Discarded</td>
<td>Smart Home System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>If the data subject plays some media other people should not know about it.</td>
<td>Discarded</td>
<td>Smart Home System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Laptops and phones should be accessible only by their owners.</td>
<td>Discarded</td>
<td>Smart Home System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>How to keep the privacy of the Wifi from the neighbours?</td>
<td>Discarded</td>
<td>Smart Home System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Does the researcher need to know the same and the address of the data subject?</td>
<td>Duplicated</td>
<td>Process</td>
<td>Third-Party</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>Do the doctor and nurse and the researchers need the same information?</td>
<td>Duplicated</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>Where we should store the information of the data subject?</td>
<td>Duplicated</td>
<td>Storage</td>
<td>Cloud</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>How can we store the information in a safe way?</td>
<td>Valid</td>
<td>Storage</td>
<td>Cloud</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>Do we need to encrypt the information?</td>
<td>Duplicated</td>
<td>Storage</td>
<td>Cloud</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Is it possible ways the glucose sensor could invade the privacy of the data subject? How to avoid it?</td>
<td>Valid</td>
<td>Device</td>
<td>Reading Sensor</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>What information could be included in the report without invading the data subject's privacy?</td>
<td>Duplicated</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>What information should be shared to the doctors and nurses?</td>
<td>Duplicated</td>
<td>Process</td>
<td>Share</td>
<td>Health Care System</td>
</tr>
<tr>
<td>3</td>
<td>Are there standard measures for each sensor to protect the data subject’s privacy? (ex: camera)?</td>
<td>Valid Device Camera Smart Home System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a gdprtext:Activity. ?Activity parrot:entails ?PrivacyPattern. FILTER (?Activity = parrot:Choose_Data) }</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Is there a way for the data subject to control the data collection frequency or the amount of information collected? Can he turn some features on and off?</td>
<td>Valid Regulations Control Smart Home System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a gdprtext:Activity. ?Activity parrot:entails ?PrivacyPattern. FILTER ('?Activity = parrot:Data_activity') }</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Are there special sensors that are more sensitive to be used in the bed rooms?</td>
<td>Not available Device Reading Sensor Smart Home System</td>
<td>SELECT ?Device ?PrivacyPattern WHERE { ?Device a parrot:Device. ?Device parrot:entails ?PrivacyPattern. FILTER (?Device = parrot:Camera) }</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Is there a way to protect the privacy by the design of the hardware? (ex: the laptop’s camera with a cover)</td>
<td>Not available Device Reading Sensor Smart Home System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a gdprtext:Activity. ?Activity parrot:entails ?PrivacyPattern. FILTER (?Activity = parrot:Data_activity) }</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>What are the privacy-preserving measurements to protect the privacy of people who did not provide consent (ex: pedestrians, visitors)</td>
<td>Not available Regulations Agreement Smart Home System</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a gdprtext:Activity. ?Activity parrot:entails ?PrivacyPattern. FILTER (?Activity = parrot:Data_activity) }</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Status</td>
<td>Storage</td>
<td>Cloud</td>
<td>System</td>
<td>Pattern</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Should the information be encrypted?</td>
<td>Not available</td>
<td>Storage</td>
<td>Cloud</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>What can be done to make sure no one else has access to data subject’s information?</td>
<td>Valid</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Real Tracking Location System (RTLS)</td>
<td>SELECT ?Activity ?PrivacyPattern WHERE { ?Activity a gdpr:Compliance. ?Activity parrot:entails ?PrivacyPattern. FILTER (?Activity = parrot:Non-authorized_people_access) }</td>
</tr>
<tr>
<td>Will the taken photos will be encrypted?</td>
<td>Duplicated</td>
<td>Storage</td>
<td>Cloud</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>For how long can we keep the photo?</td>
<td>Duplicated</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Where the photos should be stored?</td>
<td>Duplicated</td>
<td>Storage</td>
<td>Cloud</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Does the system use detection tools?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who has access to the monitoring screen?</td>
<td>Valid</td>
<td>Process</td>
<td>Access</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Does everybody has access to the API?</td>
<td>Valid</td>
<td>Process</td>
<td>Access</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Do park visitors know that their photos will be taken?</td>
<td>Valid</td>
<td>Regulations</td>
<td>Agreement</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>How to apply the GDPR rules?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who has access to the database that keeps the photos?</td>
<td>Valid</td>
<td>Process</td>
<td>Access</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Is the cloud local or used from a third-party?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Will a report be provided to the park visitors?</td>
<td>Missing</td>
<td>Regulations</td>
<td>Agreement</td>
<td>Park Monitoring System</td>
<td></td>
</tr>
<tr>
<td>Is the data subject the only one who has access to his own information?</td>
<td>Missing</td>
<td>Process</td>
<td>Access</td>
<td>Health Care System</td>
<td></td>
</tr>
<tr>
<td>Who has access to see data subject’s information?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the data subject’s information encrypted?</td>
<td>Duplicated</td>
<td>Storage</td>
<td>Cloud</td>
<td>Health Care System</td>
<td></td>
</tr>
<tr>
<td>Who are the researchers that have a copy of the information?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the cloud local in the hospital or used from a third-party?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the glucose sensor vulnerable to get information from?</td>
<td>Discarded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For how long the information will be stored?</td>
<td>Duplicated</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Health Care System</td>
<td></td>
</tr>
<tr>
<td>How to protect the information that is stored in the cloud?</td>
<td>Duplicated</td>
<td>Storage</td>
<td>Cloud</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>If more than one person is using the watch, how to protect their privacy?</td>
<td>Not available</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>How to protect the information if the phone was stolen?</td>
<td>Not available</td>
<td>Regulations Agreement</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Can the phone inform the data subject if the phone was stolen?</td>
<td>Valid</td>
<td>Regulation Notify</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>What to do if the drone got hacked on its way?</td>
<td>Valid</td>
<td>Regulations Notify</td>
<td>Drone Delivery System</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>How can we deal with the video streaming? Maybe other sensors than the camera?</td>
<td>Valid</td>
<td>Data Collection Routine</td>
<td>Drone Delivery System</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>How to protect the package from getting damaged or stolen?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>How to improve the shape of the drone?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>What if the data subject did not want to use the drone delivery system with a video streaming? Maybe some lights or tag instead of the video?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>What if the controller stores the video?</td>
<td>Valid</td>
<td>Storage Cloud</td>
<td>Drone Delivery System</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Do information need to be encrypted?</td>
<td>Duplicated</td>
<td>Storage Cloud</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>For how long the information will be stored?</td>
<td>Duplicates</td>
<td>Regulation Agree</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>What information I need from the data subject?</td>
<td>Discarded</td>
<td>Data Collection Personal Information</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Can I get the date of birth of the driver to check if he has a license?</td>
<td>Missing</td>
<td>Data Collection Personal Information</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>For how long I'll save the parking locations?</td>
<td>Duplicated</td>
<td>Regulations Agreement</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>How to choose the friends?</td>
<td>Valid</td>
<td>Process Profile</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Can we get friends from the contacts list?</td>
<td>Not available</td>
<td>Process Access</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Can the data subject choose the exact data he will share?</td>
<td>Valid</td>
<td>Process Share</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Can the data subject choose for which friend he can share his data instead of all of them?</td>
<td>Duplicated</td>
<td>Process Share</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Do we need to encrypt the information?</td>
<td>Duplicated</td>
<td>Storage Cloud</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>For how long the information will be stored?</td>
<td>Duplicated</td>
<td>Regulations Agreement</td>
<td>Fitness Watch</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Who has access to see the data subject’s information?</td>
<td>Duplicates</td>
<td>Process</td>
<td>Access</td>
<td>Fitness</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>6</td>
<td>Do we need to have a life stream of the whole journey?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>If the Drone got lost, how to protect the data subject’s information?</td>
<td>Not available</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Drone Delivery System</td>
</tr>
<tr>
<td>6</td>
<td>How to hide the content of the package from the seen?</td>
<td>Not available</td>
<td>Regulations Agreement</td>
<td>Drone Delivery System</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Do the communication needs to be encrypted?</td>
<td>Duplicates</td>
<td>Process</td>
<td>Route</td>
<td>Drone Delivery System</td>
</tr>
<tr>
<td>6</td>
<td>What exact information do we need?</td>
<td>Discarded</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Drone Delivery System</td>
</tr>
<tr>
<td>6</td>
<td>Will the information be deleted? And the orders?</td>
<td>Duplicates</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Drone Delivery System</td>
</tr>
<tr>
<td>6</td>
<td>Can we collect the information anonymously?</td>
<td>Valid</td>
<td>Data Collection</td>
<td>Personal Information</td>
<td>Drone Delivery System</td>
</tr>
<tr>
<td>7</td>
<td>If I got the cloud that I use from a third party, will they have access to the data I have?</td>
<td>Duplicates</td>
<td>Process</td>
<td>Third-Party</td>
<td>Real Tracking Location System (RTLS)</td>
</tr>
<tr>
<td>7</td>
<td>What to do in case of the router got attacked?</td>
<td>Valid</td>
<td>Regulations Notify</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>What data that could be shared with a friend?</td>
<td>Duplicates</td>
<td>Regulation</td>
<td>Control</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>Can the third party who provides the cloud server access the data that I have?</td>
<td>Duplicates</td>
<td>Process</td>
<td>Third-Party</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>For how long can we store the data?</td>
<td>Duplicates</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>How can I guarantee that the data are permanently deleted in the cloud server and there is no other copy?</td>
<td>Duplicates</td>
<td>Regulation</td>
<td>Agreement</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>What information we need from the data subject to sign up?</td>
<td>Valid</td>
<td>Process</td>
<td>Profile</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>What restrictions should be on sharing the data subject’s achievements with friends?</td>
<td>Duplicates</td>
<td>Process</td>
<td>Share</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>Is there a third party that collects and analyzes the data?</td>
<td>Discarded</td>
<td>Process</td>
<td>Third-Party</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>How to guarantee that the company provides the devices don’t have access to the data?</td>
<td>Not available</td>
<td>Regulations Agreement</td>
<td>Fitness</td>
<td>Watch</td>
</tr>
<tr>
<td>7</td>
<td>Are the data encrypted?</td>
<td>Duplicates</td>
<td>Storage</td>
<td>Cloud</td>
<td>Fitness</td>
</tr>
<tr>
<td>7</td>
<td>After the delivery, will the information (package and personal data) be saved?</td>
<td>Duplicates</td>
<td>Storage</td>
<td>Cloud</td>
<td>Drone Delivery System</td>
</tr>
<tr>
<td>7</td>
<td>Will the third party (the cloud provider) have access to the data and analyse it?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>What does the service provider (delivery company) need to deliver the packages?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>How to deal with the live streaming which violates the privacy of the data subject and the people in the way?</td>
<td>Not available</td>
<td>Regulation Agreement</td>
<td>Drone Delivery System</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Will the live streaming be saved?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Does the system require pattern recognition (face recognition, fingerprint) to be secure?</td>
<td>Discarded</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Will the history information be deleted immediately?</td>
<td>Duplicated Regulations Agreement</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Can we remove the history function in the system? Is the system going to be valuable?</td>
<td>Discarded</td>
<td>Real Tracking Location System (RTLS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>We can send a sign for someone or the emergency services if the user feels unsafe.</td>
<td>Duplicated Process Third Party Fitness Watch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>We can add a pattern recognition layer before accessing the information or achievements.</td>
<td>Discarded</td>
<td>Fitness Watch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>How to control the information that will be shared to a friend?</td>
<td>Duplicated Regulations Control</td>
<td>Fitness Watch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>How to secure the personal information from the controller (in bank account etc.)</td>
<td>Missing Regulation Agreement</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>A consent should be taken from all the neighborhood.</td>
<td>Duplicated Regulations Agreement Drone Delivery System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>How to protect the neighborhood privacy from the controller?</td>
<td>Not available</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Is the information of the live streaming going to be saved?</td>
<td>Discarded</td>
<td>Drone Delivery System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Will the live streaming be deleted if it got saved?</td>
<td>Duplicated Regulations Agreement Drone Delivery System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>How to ensure the system will not reveal the existence of the user in the house by the sensors?</td>
<td>Duplicated Regulations Agreement Smart Home System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Do we need any encryption techniques for the communication between the devices?</td>
<td>Duplicated Process Route Smart Home System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>How much of data are we going to store in the cloud?</td>
<td>Duplicated Storage Cloud Smart Home System</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```sparql
```

---

```sparql
```

---

```sparql
```

---

```sparql
```

---

```sparql
```

---

```sparql
```
### 9. How much information can we store in the gateway and in the cloud?

- **Valid Storage Cloud**
  - Smart Home System

### 9. Where the data are going to be processed? In the gateway or the cloud?

- **Missing Process Route**
  - Smart Home System

### 9. How much sensitive information is sent between the devices and the control tablet? Are there any protocols to be applied here?

- **Duplicated Process Route**
  - Smart Home System

### 9. Can we control the data to be collected by the camera? For example density of the faces of people?

- **Valid**
  - Park Monitoring System

### 9. Does the camera has a storage? Will the pictures be stored in the camera or deleted in the same time?

- **Duplicated Storage Local**
  - Park Monitoring System

### 9. What kind of information are going to be sent from the camera to the cloud?

- **Missing Process Route**
  - Park Monitoring System

### 9. Do we have a consent from the visitor?

- **Missing Regulations Privacy Policy**
  - Park Monitoring System

### 9. What information are going to be stored in the cloud that will provide the right functionality but without having unnecessary information?

- **Duplicated Storage Cloud**
  - Park Monitoring System

### 9. What information is going to be displayed to the monitoring edge? Is it faces or numbers?

- **Duplicated Storage Cloud**
  - Park Monitoring System

### 10. Does the camera open the door for the people live in the home?

- **Discarded**
  - Smart Home System

### 10. Does the tablet show personal information? Ex: the usage of the light.

- **Discarded**
  - Smart Home System

### 10. Can anyone use the control tablet and access the information?

- **Discarded**
  - Smart Home System

### 10. What about privacy in the TV?

- **Duplicated Device Reading Sensor**
  - Smart Home System

### 10. If there is a subscription in the TV like amazon extension?

- **Discarded**
  - Smart Home System

### 10. Is there any privacy procedure that can protect the information on the TV?

- **Duplicated Device Reading Sensor**
  - Smart Home System

### 10. How will the company verify my identity for sending me the bill information?

- **Discarded**
  - Smart Home System

### 10. How can I know if my information is protected from a third party?

- **Duplicated Process Third-Party**
  - Smart Home System

### 10. How can I know who is going to see these pictures?

- **Duplicated Process Access**
  - Park Monitoring System

---

**SELECT ?Activity ?PrivacyPattern**

**SELECT ?Data ?PrivacyPattern**
WHERE { ?Data a gdprtext:PersonalData. ?Data parrot:entails ?PrivacyPattern. FILTER (?Data = parrot:Raw_Data) }

---

**VALID PARROT ontology technical report**

<p>| 9 | How much information can we store in the gateway and in the cloud? | Valid Storage Cloud | Smart Home System |
| 9 | Where the data are going to be processed? In the gateway or the cloud? | Missing Process Route | Smart Home System |
| 9 | How much sensitive information is sent between the devices and the control tablet? Are there any protocols to be applied here? | Duplicated Process Route | Smart Home System |
| 9 | Can we control the data to be collected by the camera? For example density of the faces of people? | Valid | Park Monitoring System |
| 9 | Does the camera has a storage? Will the pictures be stored in the camera or deleted in the same time? | Duplicated Storage Local | Park Monitoring System |
| 9 | What kind of information are going to be sent from the camera to the cloud? | Missing Process Route | Park Monitoring System |
| 9 | Do we have a consent from the visitor? | Missing Regulations Privacy Policy | Park Monitoring System |
| 9 | What information are going to be stored in the cloud that will provide the right functionality but without having unnecessary information? | Duplicated Storage Cloud | Park Monitoring System |
| 9 | What information is going to be displayed to the monitoring edge? Is it faces or numbers? | Duplicated Storage Cloud | Park Monitoring System |
| 9 | Are we going to store the information in the monitoring edge? | Duplicated Storage Cloud | Park Monitoring System |
| 9 | For how long the information will be stored? | Duplicated Storage Cloud | Park Monitoring System |
| 9 | Who can access the monitoring edge? | Duplicated Process Access | Park Monitoring System |
| 9 | Will the pictures be used for other purposes? Ex: security or in case of a prime? | Duplicated Process Third-Party | Park Monitoring System |
| 9 | Can we get the same functionality (predict waiting time) by having less information? | Discarded | Park Monitoring System |
| 9 | What measures should be applied in the case of attack? | Duplicated Regulations Notify | Park Monitoring System |
| 10 | Does the camera open the door for the people live in the home? | Discarded | Smart Home System |
| 10 | Does the tablet show personal information? Ex: the usage of the light. | Discarded | Smart Home System |
| 10 | Can anyone use the control tablet and access the information? | Discarded | Smart Home System |
| 10 | What about privacy in the TV? | Duplicated Device Reading Sensor | Smart Home System |
| 10 | If there is a subscription in the TV like amazon extension? | Discarded | Smart Home System |
| 10 | Is there any privacy procedure that can protect the information on the TV? | Duplicated Device Reading Sensor | Smart Home System |
| 10 | How will the company verify my identity for sending me the bill information? | Discarded | Smart Home System |
| 10 | How can I know if my information is protected from a third party? | Duplicated Process Third-Party | Smart Home System |
| 10 | How can I know who is going to see these pictures? | Duplicated Process Access | Park Monitoring System |</p>
<table>
<thead>
<tr>
<th>Question</th>
<th>Discarded Data Collection Routine</th>
<th>Park Monitoring System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will a third party have access to the pictures?</td>
<td>Discarded</td>
<td>Park Monitoring System</td>
</tr>
<tr>
<td>Will pictures be attached with the time?</td>
<td>Missing Data Collection</td>
<td>Park Monitoring System</td>
</tr>
<tr>
<td>Are the pictures going to be stored with the time?</td>
<td>Duplicated Storage Cloud</td>
<td>Park Monitoring System</td>
</tr>
<tr>
<td>What privacy procedures to protect the stored information in the cloud?</td>
<td>Duplicated Storage Cloud</td>
<td>Park Monitoring System</td>
</tr>
<tr>
<td>Is there any privacy procedures for requesting and sending the pictures?</td>
<td>Duplicated Process Route</td>
<td>Park Monitoring System</td>
</tr>
</tbody>
</table>
9 Figures

9.1 Paper Figures

Figure 7: Privacy Patterns allocation of Health Care System. It shows a list of Privacy Patterns for each node in the DFD. It also shows the Privacy Patterns that should be applied across all DFD nodes.

Figure 8: Screenshot of the conducted online workshops to gather CQs that are related to a given use case DFD. The screen shots shows two use cases and the CQs found by participants.
9.2 PARROT Ontology Screenshots

Figure 9: The figure shows all the PbD schemes relationships contained in the PARROT ontology. The owl:Thing class has two sub-classes, Concept and Privacy by Design Schemes. The Privacy by Design Schemes class has five sub-classes, Principle, Guideline, Strategy, Goal, and Privacy Pattern. These five classes are also sub-classes of Concept class. Principle class has six sub-classes. The Guideline class has two sub-classes. The strategy class has one sub-class. The Goal class has one subclass.

Figure 10: The figure shows an example of an activity and the privacy patterns it entails. Thing class has Concept class which has Activity class. Activity class has Notification Activity sub-class. Notification Activity has an individual 'Notify System Attack'. This individual (activity) entails two privacy patterns, Unusual Activities and Data Breach Notification Pattern, which are individuals of Privacy Pattern class.
Figure 11: The figure shows an example of an activity and the privacy patterns it entails. Thing class has Concept class which has Activity class. Activity class has Data Activity sub-class. Data Activity class has an individual 'Choose Data'. This individual (activity) entails three privacy patterns, Negotiation of Privacy Policy, Reasonable Level of Control and Enable/Disable Function, which are individuals of Privacy Pattern class.

Figure 12: The figure shows the individuals of Personal Data class. Personal Data class is a subclass of Data.