UiA Fakultet for teknologi og realfag

IoT Assignment 1 - Privacy Impact Assessment

By

Leander Berg Thorkildsen
Cristina Torp

Supervisor:

Harsha Sandaruwan Gardiyawasam Pussewalage

Spring 2020

Faculty of Engineering and Science
Universitetet i Agder

1 Introduction

In this report, we will describe how to carry out a PIA, with focus on the life-cycle phases of the product, as well as the safety of Personally Identifiable Information (PII) and how to secure them. PIA Guidelines will be used [1][2][3], and some inspiration from the slides at school[4].

2 Life cycles

Account Creation			
Parameter	**Description/Sensitivity**	**Origin**	**User**
Username	User identifier (Not sensitive)	User	User Application server Billing service App
Password	User password (Highly sensitive)	User	User Application server Billing service App
Name, Address, Phone Number	Personal identifiable information linked to the account created. (Sensitive)	User	Application server Billing service
Age/gender	Account holder's age/gender (not sensitive)	User	Application server

Smartphone Application			
Parameter	**Description/Sensitivity**	**Origin**	**User**
Settings for the robot	Changing any settings on the robot through the application. (Not sensitive)	Application server	Smart phone application Application server
Robot Serial number	Unique identifier for the robot (Not sensitive)	Application server User	Smart phone application User Application server
Captured data	All data that is being recorded and stored in the database. (Highly sensitivity)	User	Smart phone application Application server Owner of robot

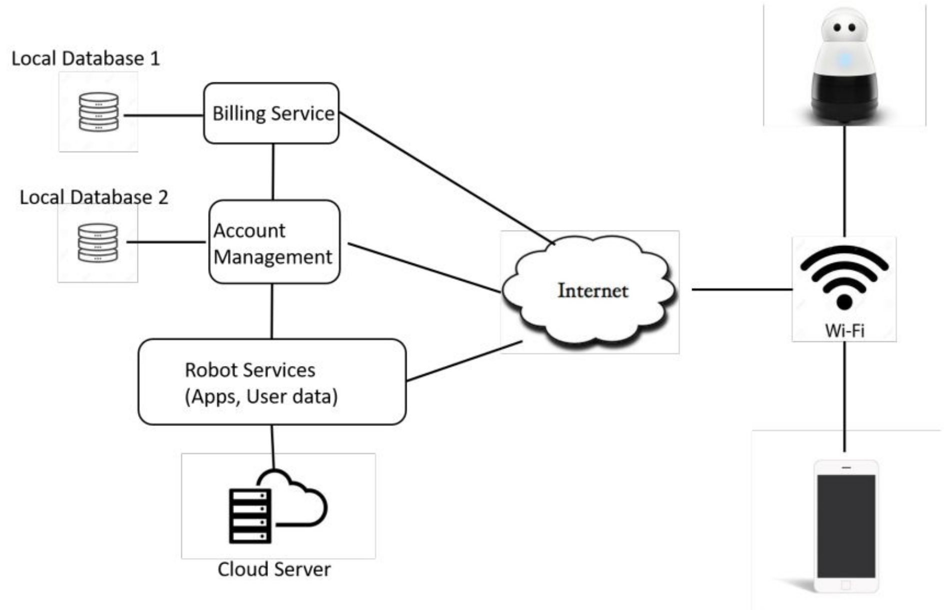
Daily Usage			
Parameter	**Description/Sensitivity**	**Origin**	**User**
Microphone data	All voice recordings (highly sensitive)	Robot	Application server and user
Camera data	Video and photos (highly sensitive)	Robot	Application server and user

3 Carrying out PIA

3.1 Identify need for PIA

The product consists of a robot connected to the home wifi that can interact with the users and provide security in their homes. By recording and capturing images, this robot will be able to function as a security camera. The big difference is that the user can interact with it through voice commands, as well as through their smartphone application. Since it is recording both images and voices of the user, this is considered highly sensitive information, and the challenge here is to ensure the users privacy is being handled correctly. [2]

3.2 Describe information flows



3.3 Identify privacy risk

Potential privacy risks can occur within multiple stages of this system. There is a smartphone application connected to the robots that can be used to keep track of applications downloaded and data recorded. This can potentially be a risk, since the captured data is accessible for the user through their phone, meaning it contains all the recorded videos, text, and images. Furthermore, the cloud provider is also potentially a risk, since they too possess the voice recordings, in the form of text transcripts. [2]

3.4 Identify privacy solutions

A privacy solution can be to implement policies to ensure that the collected data is being properly anonymoused or deleted. This can mean that the different applications in this system will not keep data for longer than potentially needed. The current data collected from the robot is. How data is stored is also something to consider, with up-to-date encryption being a solution. [2]

3.5 Record PIA outcomes, and sign-off

This last step is basically a formality when it comes to business. The final report is signed off, containing the status of each risk.

4 Resources

[1] *"Privacy Impact Assessment Toolkit"* - Privacy Commissioner (July 2015)
https://www.privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Part-1.pdf

[2] *"Part 2: How to do a privacy impact assessment (PIA)"*
https://www.privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Assessment-Part-2-FA.pdf

[3] "PIA Guide" - Information and Privacy Commission (May 2015)
https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf

[4] Presentation slides