Internet of Things Privacy Infrastructure*

Daniel Smullen, Justin Donnell, Yuanyuan Feng, Gaurav Misra, Norman Sadeh

Overview

Every day, new smart devices, sensors, smart systems, home automation, and data collection systems are released onto the market and deployed. We refer to these Internet of Things (IoT) connected devices, services, and so on as *IoT resources*.

Today, IoT resources are being deployed in the spaces we frequent – often without our knowledge or consent. New regulatory regimes (such as GDPR in Europe) mandate that data collectors must provide users with the ability to consent to the data collection practices, and must notify users about many specifics.

The Internet of Things Privacy Infrastructure* has been deployed on two university campuses: Carnegie Mellon University, and University of California, Irvine.

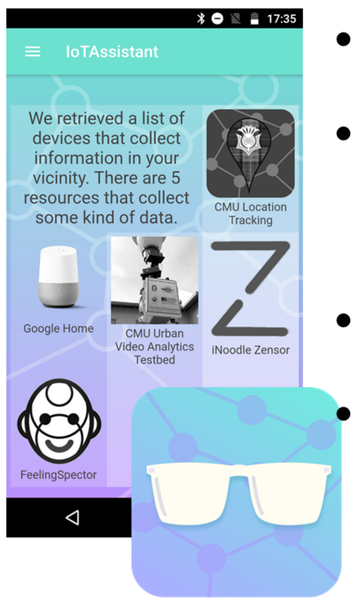
We are developing and piloting an Internet of Things Privacy Infrastructure, capable of:

1. *Notifying people about the existence of IoT resources in their vicinity, describing their data practices in a simple and understandable privacy notice.*
2. *Providing control options for people to change how they engage with the IoT resources around them.*
3. *Providing ways for IoT resource owners, operators, and administrators to provide access to settings and facilities, helping their data collection practices and IoT resources to maintain compliance with the law.*

Read our recent article, "Personalized Privacy Assistants for the Internet of Things“ In IEEE Pervasive Computing: Special Issue - Securing the IoT, April 2018

We are looking for more institutions who would like to have our infrastructure deployed at their location.

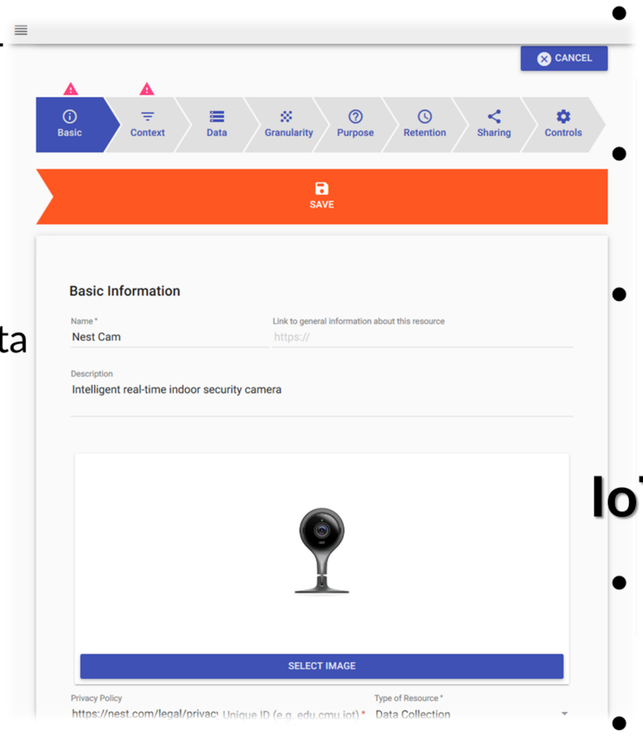
IoT Assistant App



- Browser for the Internet of Things.
- Helps users discover IoT resources in their physical location and vicinity.
- Provides notice about data collection activities
- Offers control options, such as opt-out, data erasure, and others (where available).

IoT Resource Registries (IRRs)

- Stores and retrieves information about IoT resources in a particular location.
- Provides a wizard to define the resources which exist in that location, and what data collection practices they perform.
- Can be operated, administrated, and curated by any organization – even individuals.



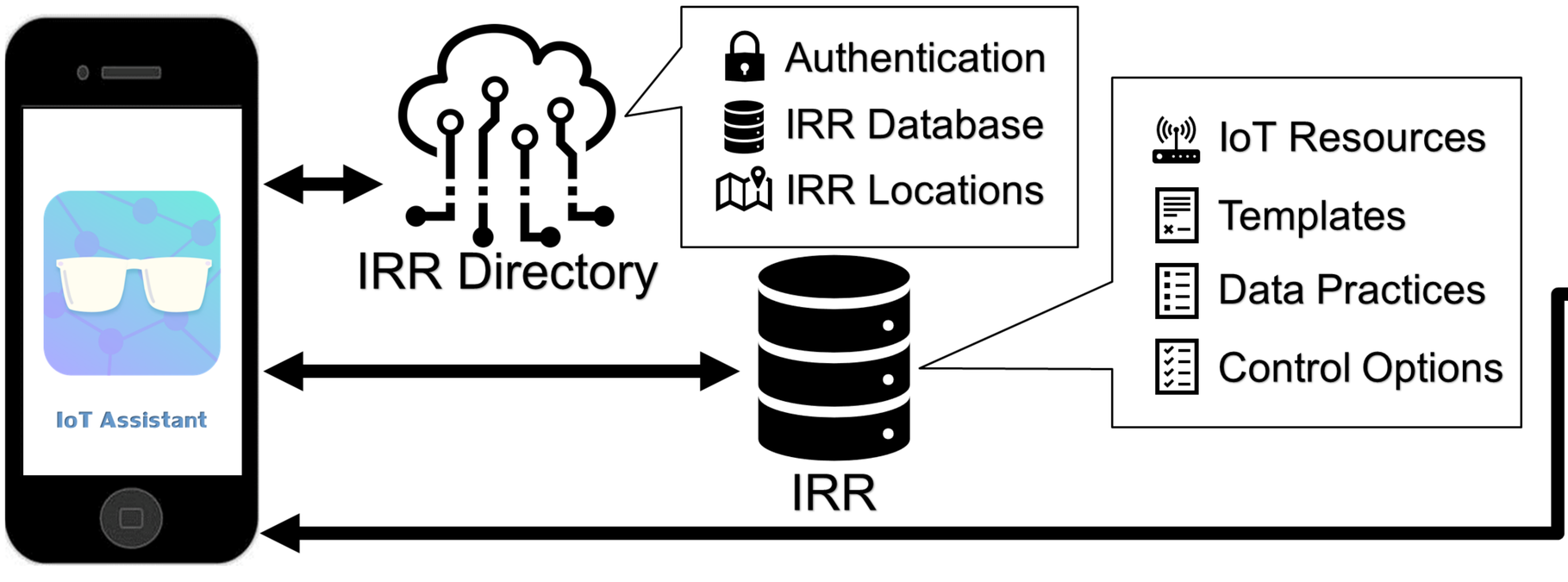
IRR Directory

- Helps IoT Assistants pair their users with IRRs relevant to their current location.
- Provides a single-sign-on functionality for the entire infrastructure.
- Maintains the authoritative records on what IRRs exist, and what areas they cover.

IoT Resources

- Information about IoT resources is stored in IRRs, and browsed through the IoT Assistant app.
- We provide easy ways of defining resources using pre-filled *templates*, which contain information about off-the-shelf devices (e.g. Amazon Echo, Nest Camera)

Architecture



PI: Norman Sadeh (sadeh@cmu.edu)

www.privacyassistant.org

Carnegie Mellon University CyLab Security and Privacy Institute

* Patent Pending. This work is funded in part by the Defense Advanced Research Projects Agency Brandeis Privacy Initiative (Grant FA8750-15-2-0277) and the National Science Foundation (Grant SBE-1513957).