The Personalized Privacy Assistant for IoT Project

Lujo Bauer, Lorrie Cranor, Norman Sadeh,
Anupam Das, Martin Degeling, Sruti Bhagavatula, William Melicher, Pardis Emami Naeini, **Shikun Zhang**

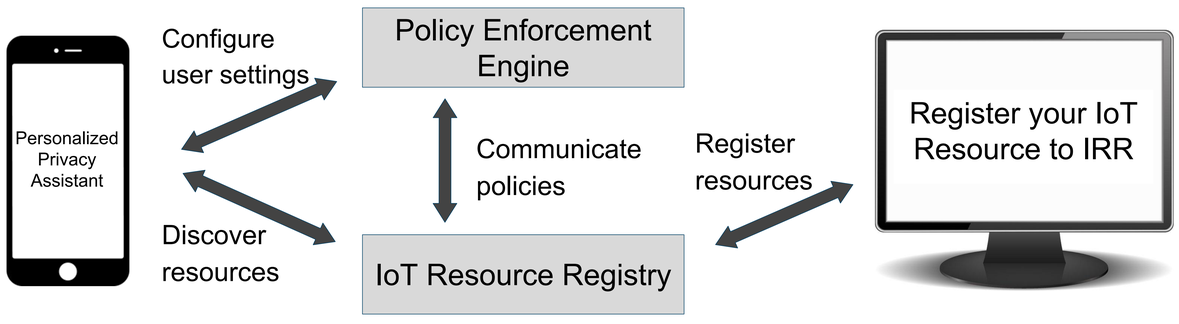
Carnegie Mellon University
www.privacyassistant.org

About the Project

We envision **personalized privacy assistants** as intelligent agents capable of learning the privacy preferences of their users and at times semi-automatically making many privacy decisions on their behalf.

This requires an infrastructure to communicate privacy policies between environments. We developed a machine readable privacy policy language for IoT and a web application for conveying the policy to users. Our IoT Assistant understands these policies and visualizes them in a mobile app.

IoT Infrastructure (Simplified)



Policy Language for IoT

Our policy language is implemented as a JSON Schema v4. It specifies necessary elements to describe IoT resources and services. It is both human and machine readable.

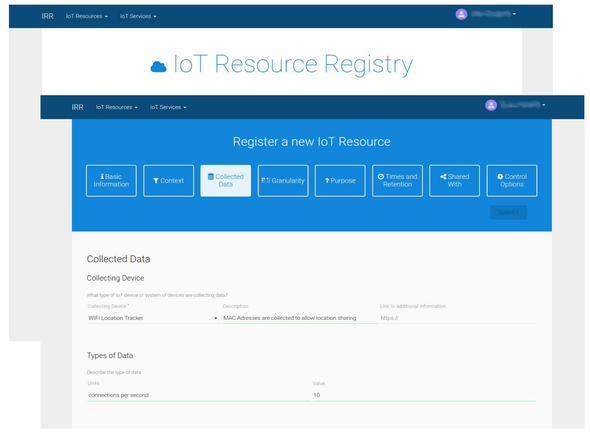
```
"contextType":{
  "id": "#contextType",
  "properties": {
    "location": {
      "description": "Where does data collection take place and who is responsible for that",
      "$ref": "#/definitions/locationType"
    },
    "operator": {
      "description": "What organization/individual owns and operates the devices?",
      "$ref": "#/definitions/informationType"
    },
    "collector": {
      "description":"What type of IoT device or system of devices are collecting data?",
      "$ref": "#/definitions/collectorType"
    },
    "time": {
      "description": "During which time period (day/week/month etc) does data collection take place?",
      "type": "array",
      "items": {"$ref": "#/definitions/timeType"}
    },
    "granularity": {
      "description": "When the data is being collected, in what form is it collected?",
      "$ref": "#/definitions/granularityType"
    }
  },
  "required": ["collector"]
}
```

IoT Resource Registry

Web application that can be set up in any IoT environment.

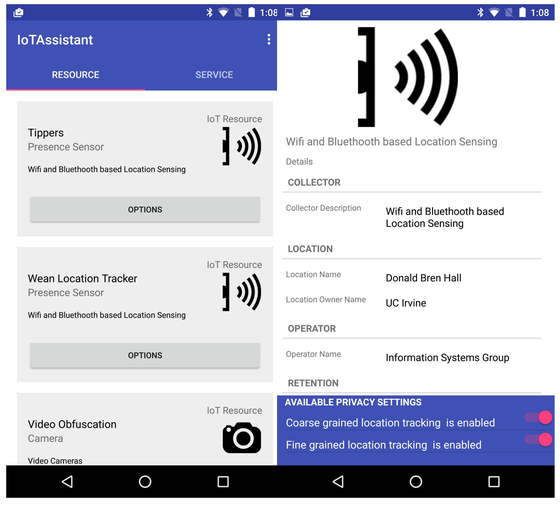
Those responsible for setting up IoT devices can register their resource, specify what the data is collected, how data is processed, how long data is stored and which control choices (REST APIs) are available to users.

The IRR is advertised with Bluetooth beacons that can be discovered by the IoTA.



The IRR is build on the open MEAN Platform (MongoDB, ExpressJS, Angular, NodeJS) and allows authentication with any OAuth provider.

IoT Assistant



The Internet of Things Assistant (IoTA) discovers IRRs via Bluetooth and renders the privacy policy language in an easy to use interface.

Users can learn about nearby resources and services, download and use the services. The IoTA emphasizes the choices available (like opting out or in or choose other variants of data collection).

In the future the IoTA will be able to learn users' preferences and apply them semi-automatically.

Acknowledgement

Our research is generously supported by DARPA, Air Force Research Laboratory, Google