# Personalized Privacy Assistant for IoT

**Norman Sadeh, Martin Degeling, Anupam Das, Aerin Shikun Zhang,
Alessandro Acquisti, Lujo Bauer, Lorrie Cranor, Anupam Datta, Daniel Smullen**

## Overview

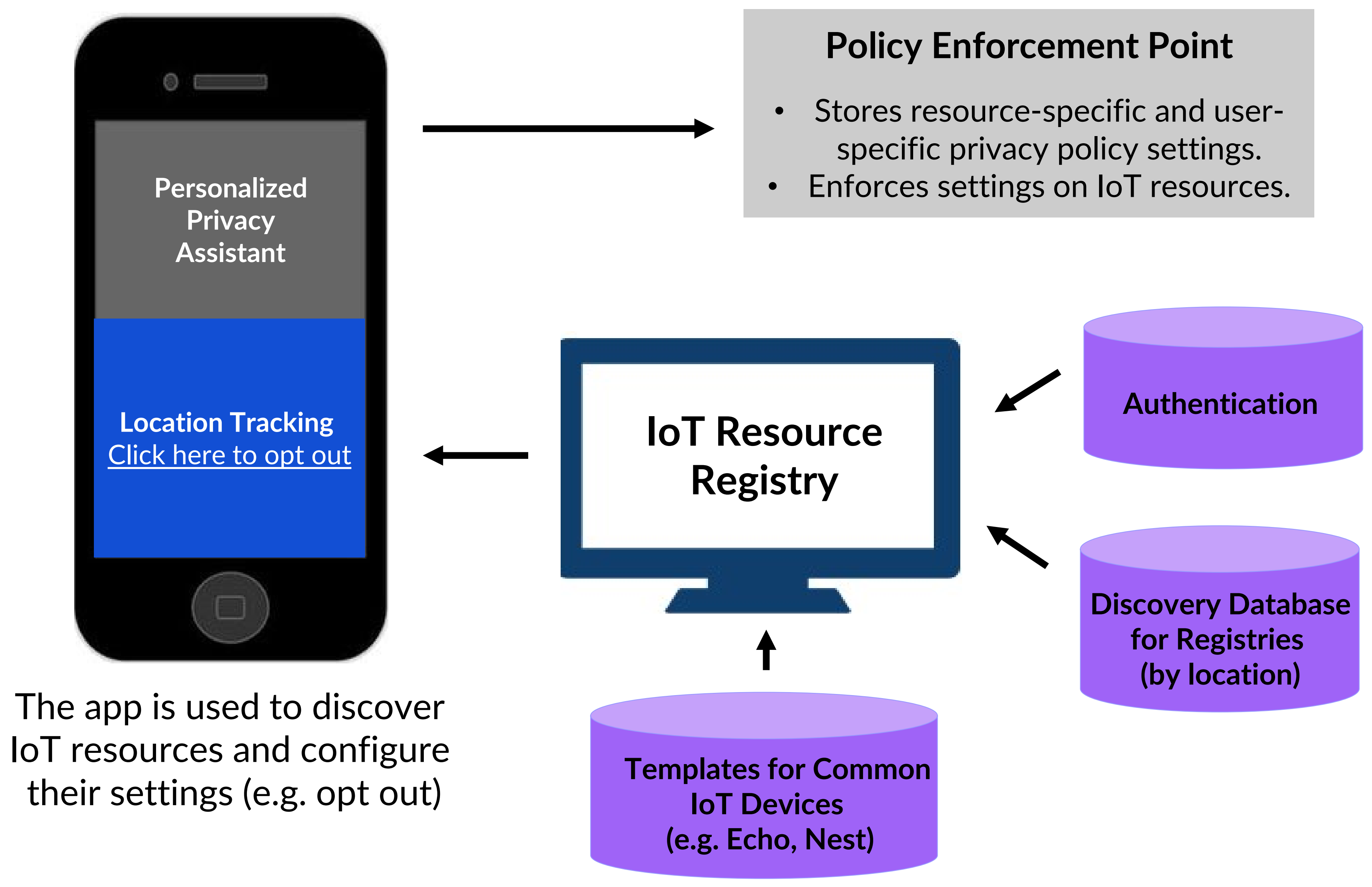
The Internet of Things (IoT) and Big Data are making it impractical for people to keep up with the expanding ways their data is collected. A new, more scalable paradigm that empowers users to regain control over their data is needed. We are developing and piloting **Personalized Privacy Assistants**, capable of:

- *Selectively notifying users about practices relevant to them.*
- *Helping to configure settings based on users' preferences.*
- *Learning the privacy preferences of users.*

**IoT Resource Registries** are new infrastructure used by Privacy Assistants to aid people in the discovery and usage of IoT-connected resources (e.g. sensors, services, apps) that are collecting and processing data in your vicinity.

A first version of the Personalized Privacy Assistant app and infrastructure has been deployed on two university campuses.

## Infrastructure



Personalized Privacy Assistant

Location Tracking
Click here to opt out

The app is used to discover IoT resources and configure their settings (e.g. opt out)

**Policy Enforcement Point**

- Stores resource-specific and user-specific privacy policy settings.
- Enforces settings on IoT resources.

IoT Resource Registry

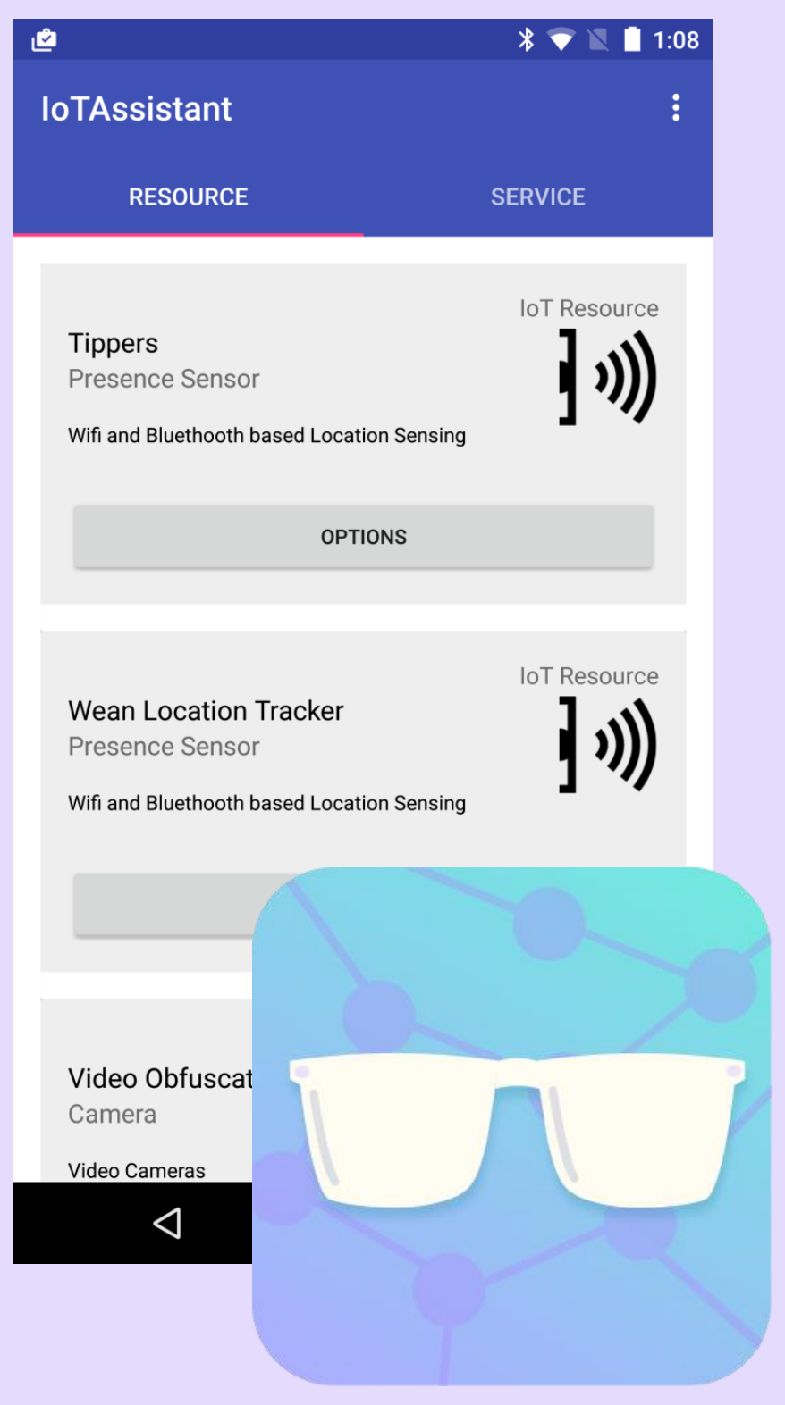
Authentication

Discovery Database for Registries (by location)

Templates for Common IoT Devices (e.g. Echo, Nest)

## Components

### Privacy Assistant



IoTAssistant

RESOURCE | SERVICE

Tippers
Presence Sensor
Wifi and Bluetooth based Location Sensing
IoT Resource
OPTIONS

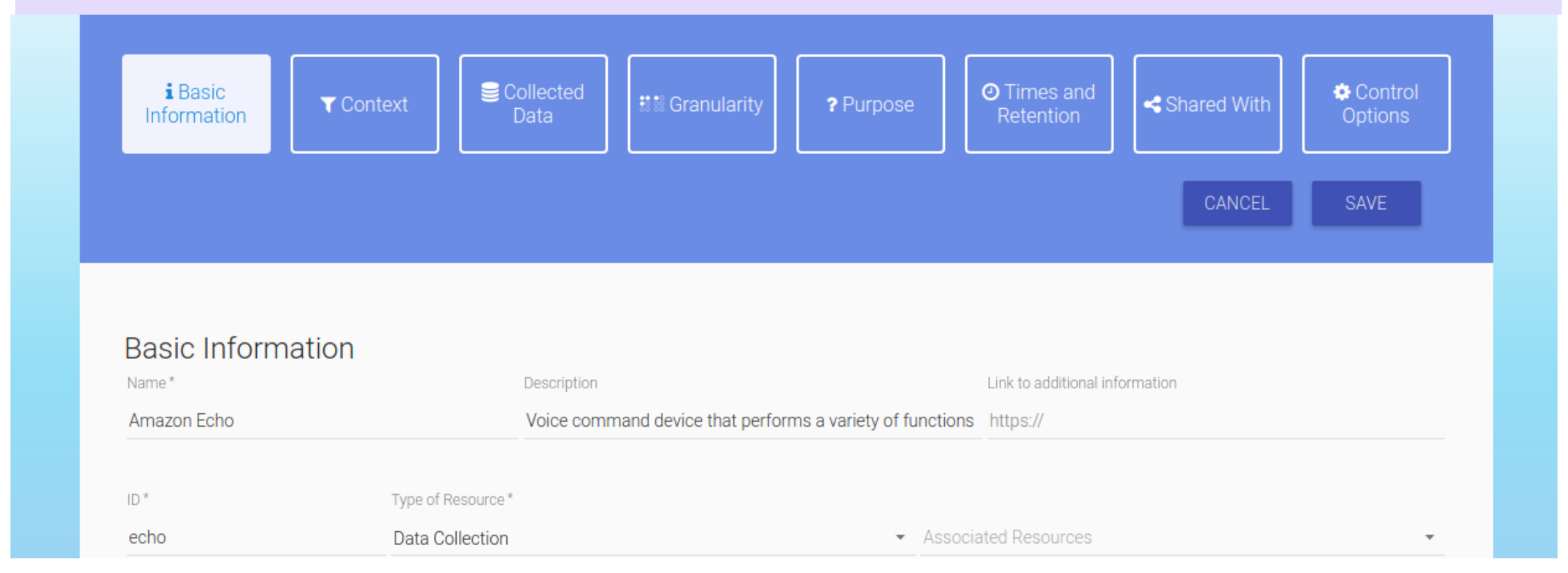
Wean Location Tracker
Presence Sensor
Wifi and Bluetooth based Location Sensing
IoT Resource

Video Obfuscat
Camera
Video Cameras

- Helps users discover IoT resources in their vicinity.
- Displays resources' privacy polices.
- Offers resource configuration options, simplifying privacy choices.

### IoT Resource Registries

- Hosted platform.
- Stores and retrieves registered resources, policies, capabilities.
- Curated by resource owners and registry administrators.



Basic Information

Name *: Amazon Echo

Description: Voice command device that performs a variety of functions

Link to additional information: https://

ID *: echo

Type of Resource *: Data Collection

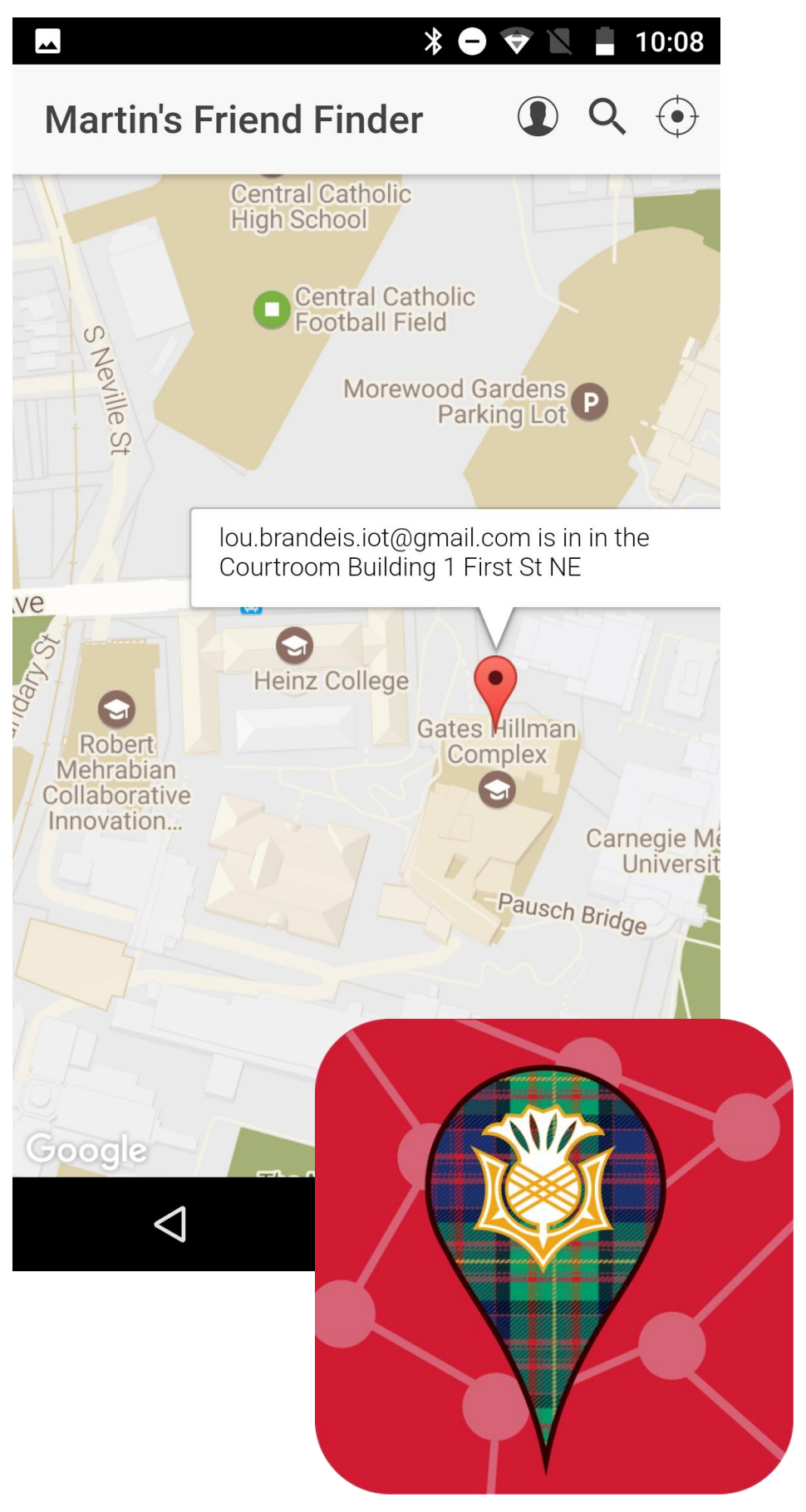
Associated Resources

### Privacy Preference Modeling

- Vignette study on IoT scenarios.
- Measured participants' comfort level, whether they would allow or deny data collection.
- Developed a prediction model for user data collection preferences.

**To find out more - see our paper:**
*Naeini, P. et. al. "Privacy Expectations and Preferences in an IoT World." SOUPS 2017*

## Applications



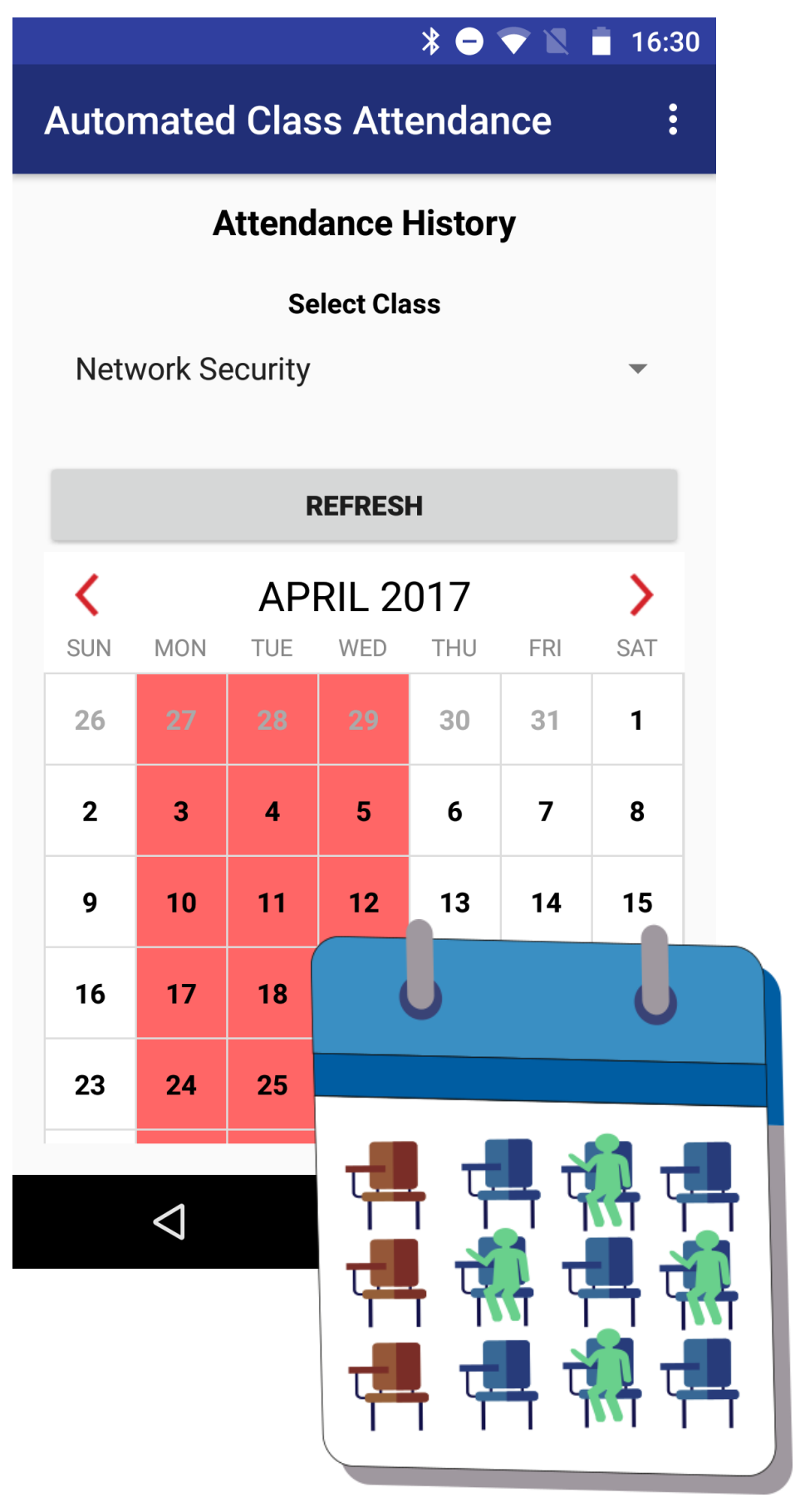
Martin's Friend Finder

lou.brandeis.iot@gmail.com is in in the Courtroom Building 1 First St NE

Central Catholic High School
Central Catholic Football Field
S Neville St
Morewood Gardens Parking Lot
Heinz College
Robert Mehrabian Collaborative Innovation...
Gates Hillman Complex
Carnegie Me Universit
Pausch Bridge
Google

### CMU Friend Finder

- Indoor location tracking for CMU campus using WiFi and Bluetooth beacons.
- Enables location sharing with friends using a map.
- Privacy Assistant integration allows users to enable or disable tracking, and configure tracking options.



Automated Class Attendance

Attendance History

Select Class

Network Security

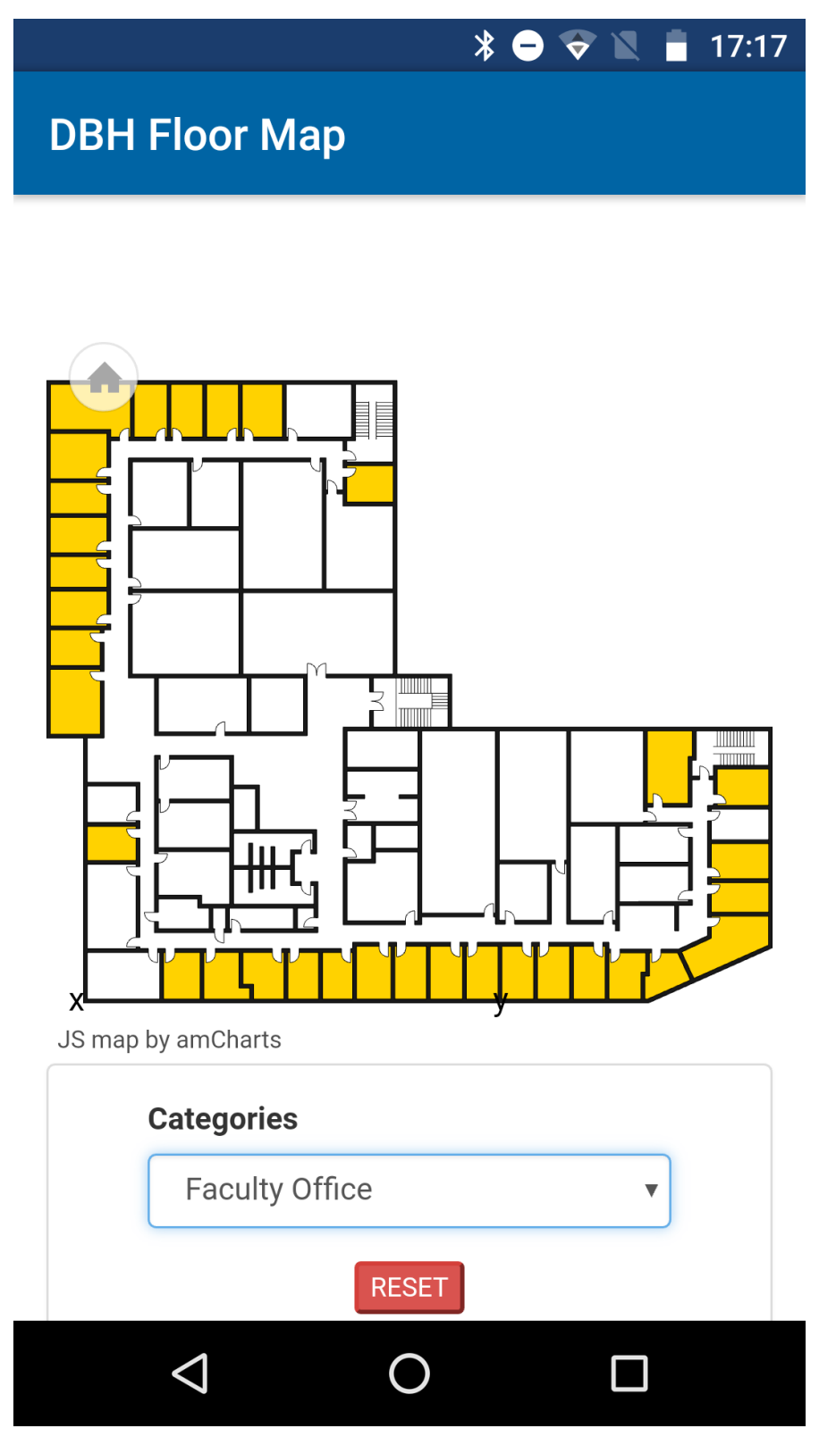
REFRESH

APRIL 2017

| SUN | MON | TUE | WED | THU | FRI | SAT |
|---|---|---|---|---|---|---|
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | | | | |
| 23 | 24 | 25 | | | | |

### Class Attendance

- Mobile application for students and teachers.
- Automatically tracks attendance using facial recognition cameras deployed in-situ.
- Privacy Assistant integration allows users to opt in or out of the service.



DBH Floor Map

Categories: Faculty Office

RESET

### Concierge

- Indoor navigation assistant for UC Irvine campus.
- Driven by customized building management system (BMS).
- Highlights local events.
- Privacy Assistant integration enables control over what data is collected by BMS.

This research has been conducted as part of the Personalized Privacy Assistant for Big Data and IoT Project at CMU.
This work is partially funded by the DARPA Brandeis Initiative.

**Contact: Norman Sadeh (sadeh@cmu.edu)**

**www.privacyassistant.org**

Carnegie Mellon University

DARPA