Personalized Privacy Assistant for IoT

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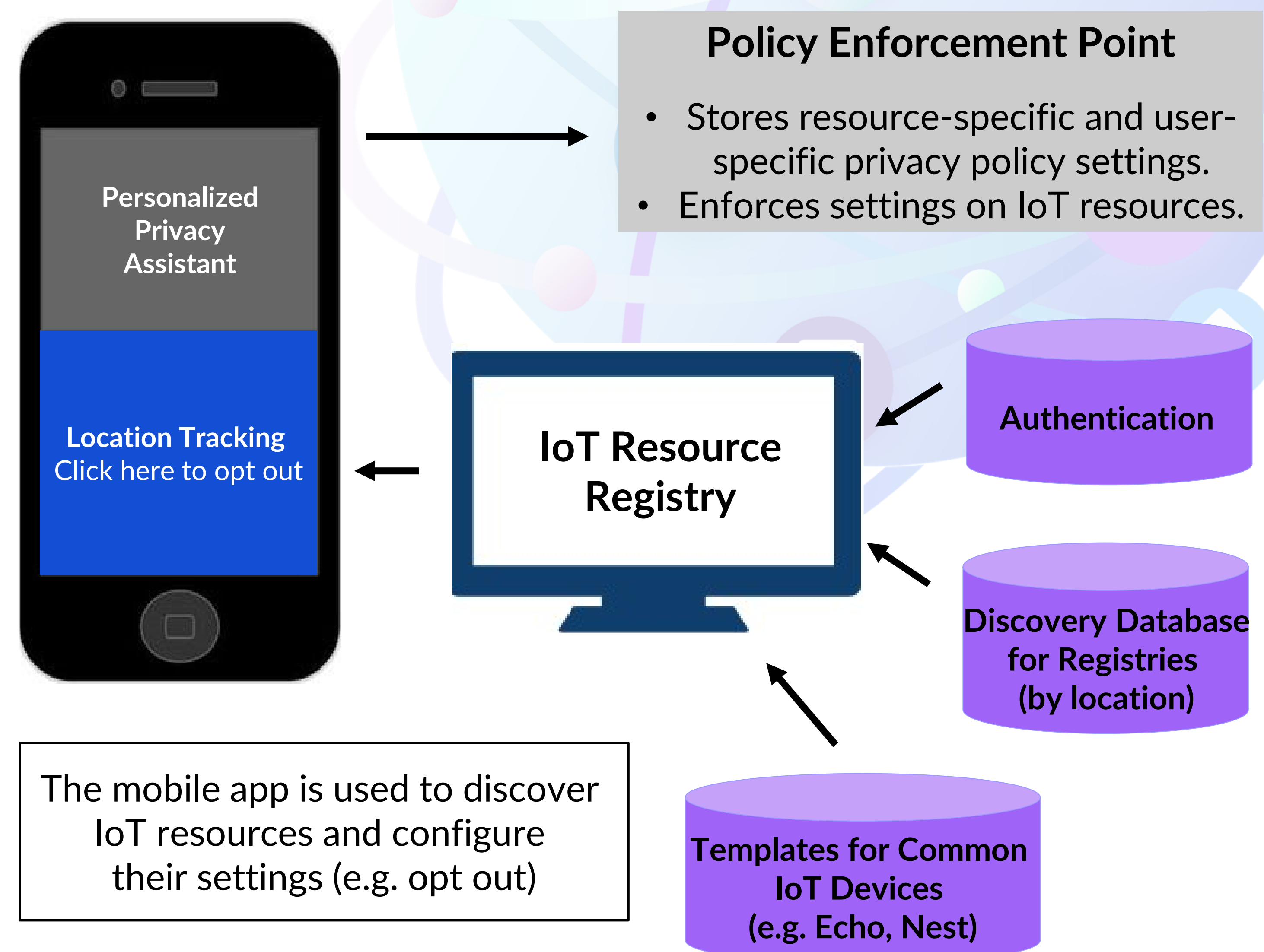
Overview

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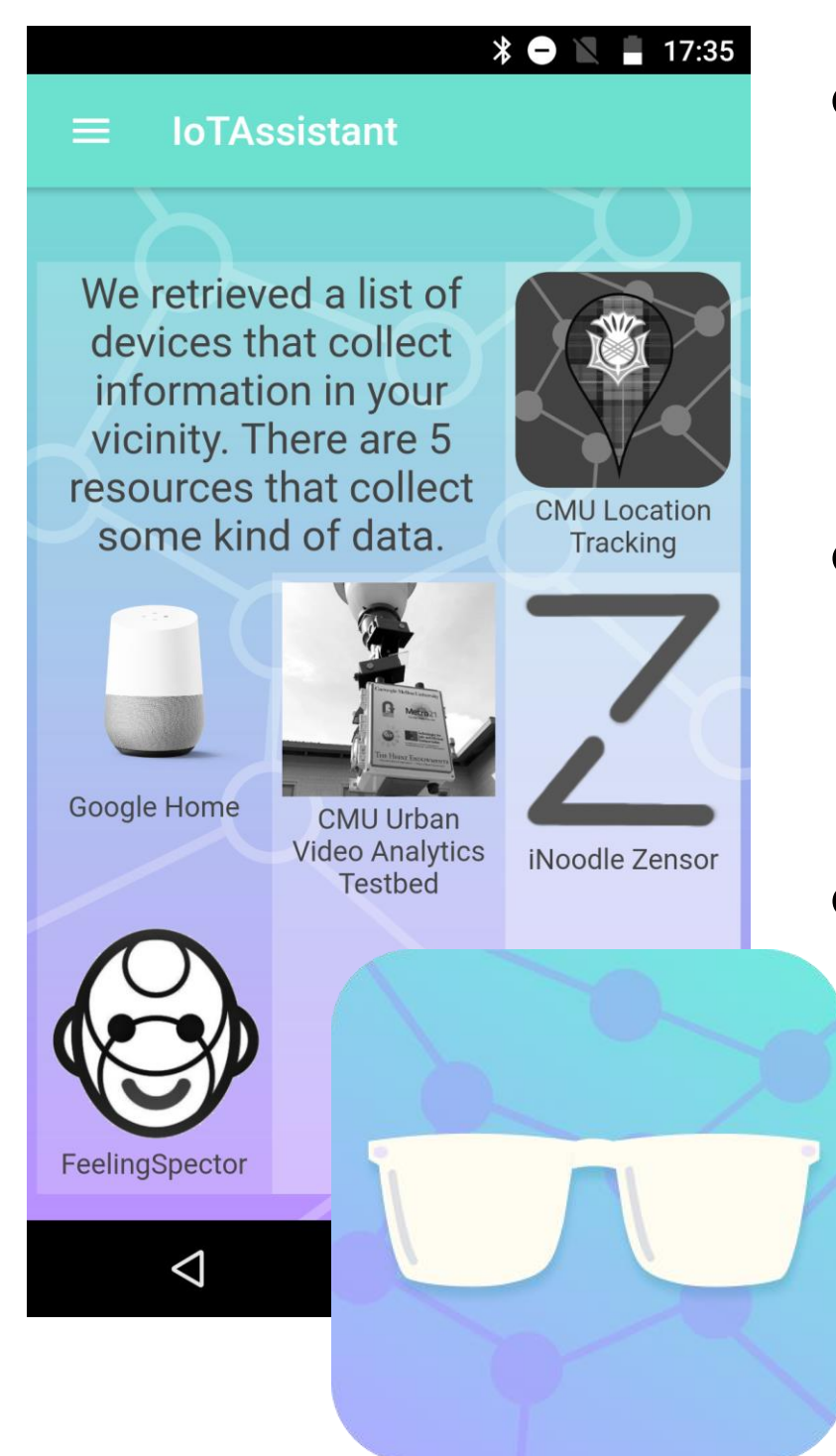
A first version of the Personalized Privacy Assistant app and infrastructure has been deployed on two university campuses.

Infrastructure

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

Personalized Privacy Assistant

Location Tracking Click here to opt out

IoT Resource Registry

Authentication

Discovery Database for Registries (by location)

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

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

Components

Privacy Assistant App

- 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.

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.

Find out more, read our papers:

A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh and M. Satyanarayanan, **"Assisting Users in a World Full of Cameras: A Privacy-aware Infrastructure for Computer Vision Applications"**, IEEE CVPRW 2017

P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor and N. Sadeh, **"Privacy Expectations and Preferences in an IoT World"**, SOUPS 2017

J. Wang, B. Amos, A. Das, P. Pillai, N. Sadeh, M. Satyanarayanan, **"A Scalable and Privacy-Aware IoT Service for Live Video Analytics"**, ACM MMSys 2017

Applications

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.
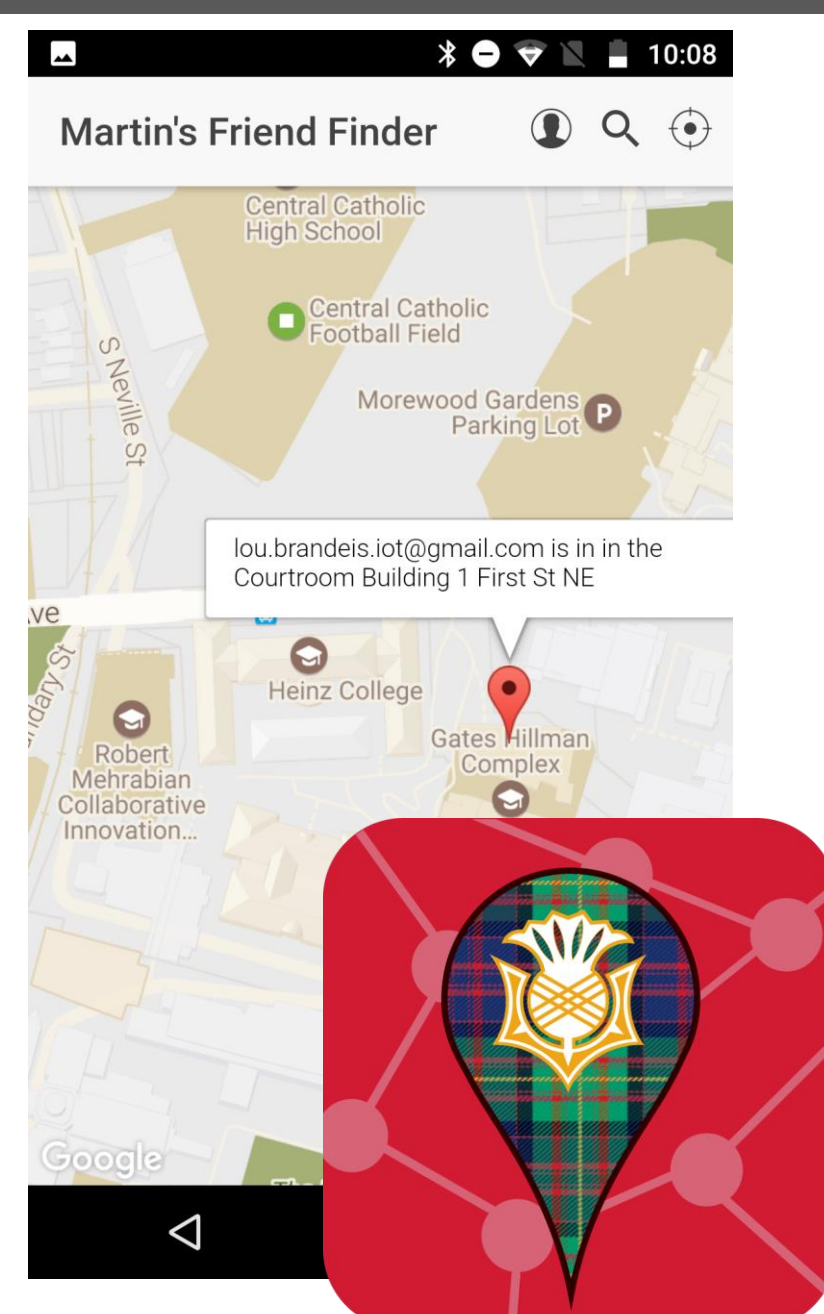
Class Attendance Tracker

- 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.
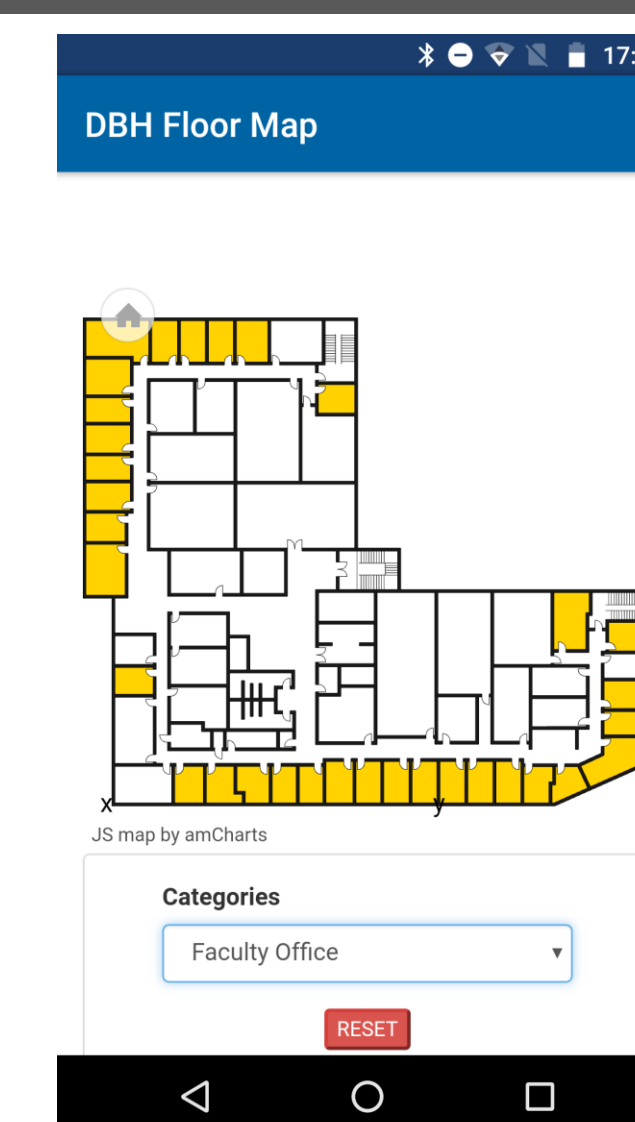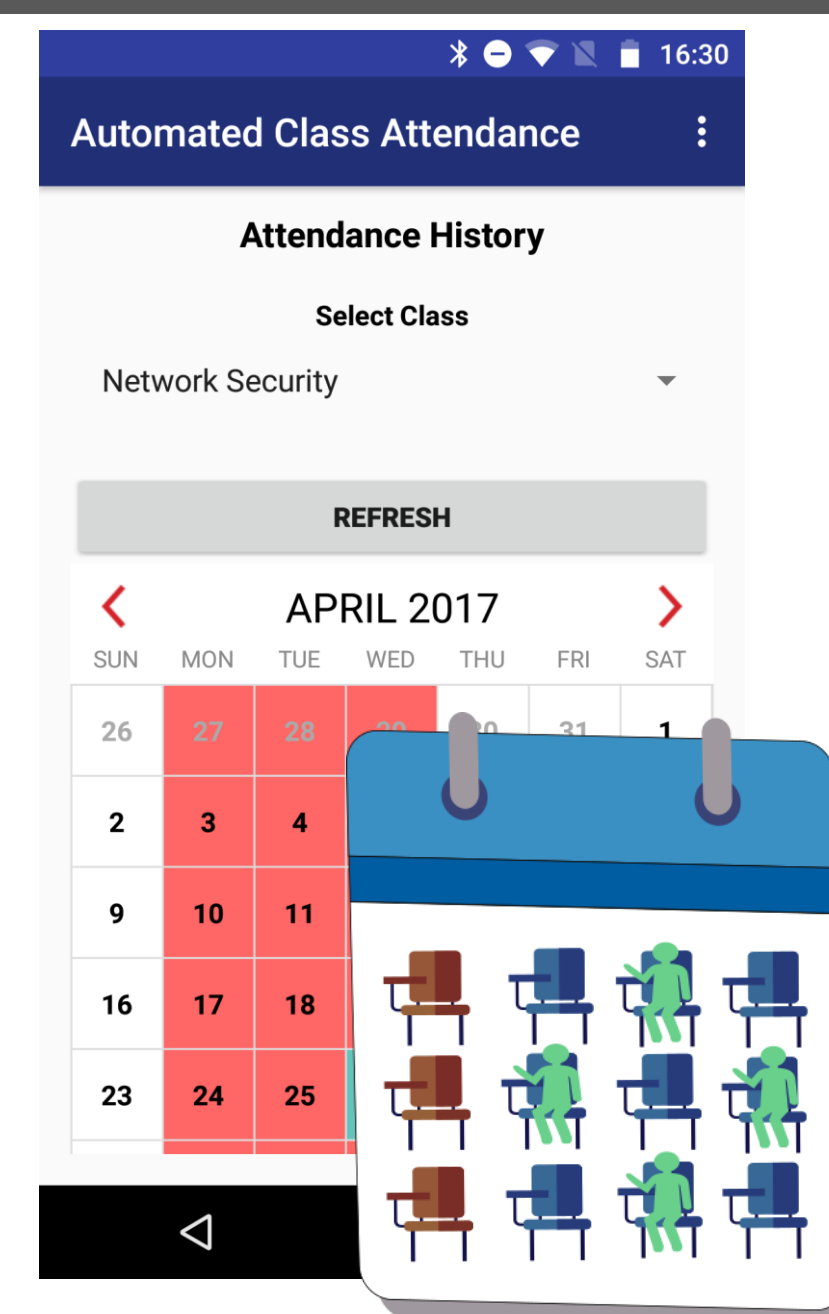
UC Irvine Concierge

- 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.

Contact: Norman Sadeh (sadeh@cmu.edu)

www.privacyassistant.org

Carnegie Mellon University

DARPA