Personalized Privacy Assistant Project: Internet of Things Assistant

Akshath Jain

Advisor
Norman Sadeh

Contributing Members
Justin Donnell, Yuanyuan Feng
Akshath Jain, Gaurav Misra

Abstract

There currently exists no mechanism for individuals to determine the presence of Internet of Things (IoT) devices around them. Moreover, the ability for individuals to understand, control, and configure how their data is collected and processed by these devices is impractical, if not impossible. And with the increasing ubiquity of IoT devices, a solution is paramount.

This is where the Internet of Things Assistant (IoTA) comes in. The IoTA is a part of the Internet of Things Privacy Infrastructure (IoTPI) — a scalable paradigm where system administrators can list all nearby IoT devices and where end-users can view, manage, and opt-in/out of data collection, empowering individuals to retake control of their data. This presentation highlights the progress made by the Personalized Privacy Assistant team in delivering a working prototype of the IoTA app.

Introduction

The primary objective of the Internet of Things Privacy Infrastructure (IoTPI) is to provide a robust mechanism by which IoT device owners and administrators can inform end-users about the presence of IoT devices deployed nearby, detail data collection / usage practices, and enable users to opt-in/out of data collection.

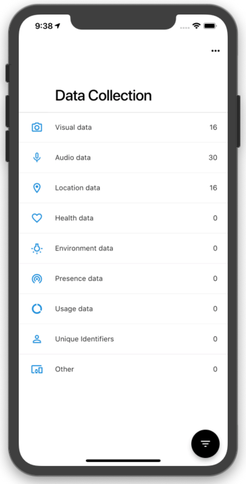
- **IoT Resource —** An IoT resource can either be a standalone IoT device (e.g. a smart speaker) or a system of IoT devices that function as a network (e.g. a surveillance system of multiple security cameras).
- **IoT Resource Listings —** An IoT resource listing is a collection of details about a particular IoT Resource, including basic information, data practices, privacy policy, and location (associated IRR).
- **IoT Resource Registries (IRR) —** An IoT resource registry is a collection of IoT Resources within a geographic area (such as a building). IRR administrators are responsible for entering all IoT resources within their IRR using the IoTPI Web Portal.
- **IRR Directory —** The IRR directory contains all IRRs. A user can query the IRR directory to discover nearby IRRs using the IoTA.
- **IoTPI Web Portal —** The interface that IRR administrators can use to create and publish IoT Resource Listings.
- **IoT Assistant Mobile App (IoTA) —** A mobile application that allows end-users to discover nearby IRRs / IoT Resources and opt-in/out of data collection. The IoTA communicates directly with the IoTPI.
- **Policy Enforcement Infrastructure —** The Policy Enforcement Infrastructure is a 3rd party system (managed by IRR Administrators) that handles opting users in/out of data collection. The IoTPI notifies the 3rd party Policy Enforcement Infrastructure that the user has opted in/out of data collection.

Technologies

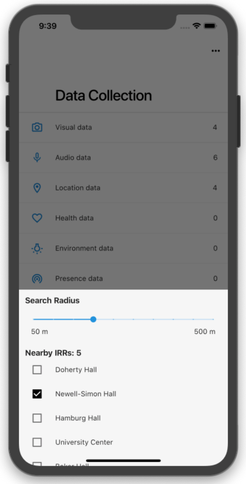
The IoTA is built using Flutter, a cross-platform UI framework designed to deliver fast, native performance on both Android and iOS. Flutter was chosen given its development efficiency and high flexibility in rendering UI components dynamically, features highly conducive to rapid prototyping and development. Flutter is based in Dart, a language with a flexible type system, JIT compilation for hot-reload capabilities, and AOT compilation for instant startup.

Utilizing a cross-platform framework gave us the added advantage of only having to maintain a single codebase for two separate versions of the app (Android and iOS). And given that Flutter compiles natively to both Android and iOS, there was no performance hit compared to developing natively.

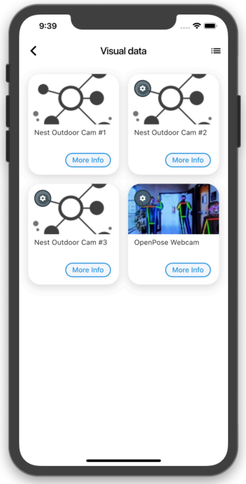
Application Flow



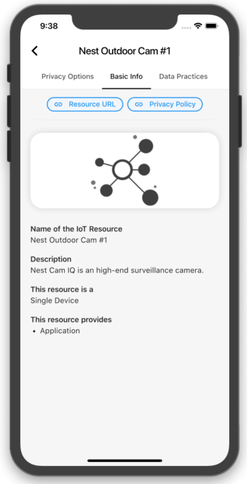
Overview screen that displays the types of data being collected by nearby resources.



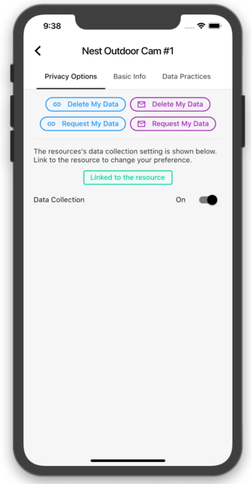
The user can refine their search parameters and filter nearby devices by IoT resource registry (IRR).



Category screen that displays all resources using a particular type of data.



Screen that displays detailed information about a particular resource and its data collection practices



If privacy options are available, the user can opt-in/out of data collection and request to download or delete their data.

Infrastructure