A Privacy Infrastructure for Notice and Choice in the Internet of Things

Norman Sadeh
Carnegie Mellon University
Pittsburgh, PA 15213, USA
sadeh@cs.cmu.edu

Yuanyuan Feng
Carnegie Mellon University
Pittsburgh, PA 15213, USA
yuanyuanfeng@cmu.edu

Justin Donnell
Carnegie Mellon University
Pittsburgh, PA 15213, USA
jdonnell@cmu.edu

Gaurav Misra
Carnegie Mellon University
Pittsburgh, PA 15213, USA
gmisra@cs.cmu.edu

Abstract

In the Internet of Things (IoT), users interact with a growing collection of resources that all rely on the collection and processing of their information. Many of these interactions take place unbeknownst to the user. A user may not notice the camera in front of which she is passing and has no ability to determine whether the camera links to facial recognition or other video analytics functionality, who the data is shared with, or for how long the data will be retained. To make matters worse, there is no practical mechanism a to expose privacy settings to users such as opt-in or opt-out settings. In this poster, we present a novel IoT privacy infrastructure designed to remedy this situation. The infrastructure enables owners of IoT resources (e.g. cameras, smart speakers, location tracking functionality, etc.) to publicize the presence of their resources. As they come within the vicinity of these IoT resources, people are able to discover their presence, their data collection and use practices, as well as any privacy choices they might make available to users. The infrastructure supports a broad range of notice and choice options, including requirements associated with regulations such as GDPR or CCPA.

Author Keywords

Privacy management; Internet of Things; usable privacy;

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

Introduction

Today, billions of IoT devices are already deployed worldwide, with many more expected over the years to come [1]. These devices collect an increasingly wide range of data about us, with this data being processed and shared in support of ever more diverse scenarios. These processes tend to take place unbeknownst to data subjects who often are unaware of the presence of the devices, have no ability to determine exactly what data is being collected, and how that data is processed. To make matters worse, there is no practical mechanism to allow users to exercise any choice over the collection and use of their data. For instance, there is no practical mechanism for users to opt in opt out of some practices, or exercise other rights such as those granted under GDPR or CCPA. In short, for all practical purposes, people have little or no control over their data in today's Internet of Things. This situation creates mistrust and is hampering adoption of these technologies [3].

We present an IoT Privacy Infrastructure$^{\text{(patent pending)}}$ (IoTPI) designed to remedy this sitation. The infrastructure enables owners of IoT technologies (e.g. cameras, smart speakers, location tracking functionality, etc.) to publicize the presence of their IoT resources to people who are nearby. As they come within the vicinity of these IoT resources, people are able to discover the their presence, including who operates them, what data they collect, what happens to that data, as well as any privacy choices made available by the resources. The IoTPI is capable of supporting a broad range of notice and choice options, including regulatory requirements associated with regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). As an additional benefit, the IoTPI also lends itself to the development of Personalized Privacy Assistants that can assist users in managing their privacy, from customizing notification mechanisms and only informing users about resources and practices they would want to be notified about, to helping them manage what we expect to be a growing collection of privacy choices based on models of their preferences (e.g. see [4] for an example of such an assistant developed to help smartphone users manage their mobile app permission settings).

System Architecture

The IoTPI enables IoT device owners/administrators to inform the public about the presence of their *IoT resources*. An "IoT resource" can be a single IoT device that functions independently (e.g., a smart doorbell, a smart speaker) or a system of connected IoT devices/sensors that function as a whole with some form of centralized control (e.g., a security system comprised of surveillance cameras and door access controls). The owner/administrator of the IoT resource can create a description of the resource and advertise its presence in one or more registries - in the form of an *IoT Resource Listing*. A resource listing typically includes the name of the resource, its area of coverage (namely the area within which it collects data), its data practices (e.g., types of data being collected, purpose of data collection), and any available privacy options made available to people such as the ability to opt in or out of some practices, the ability request that their data be erased, and more). While the IoTPI has been designed to support a rich set of data practices, as required to support regulations such as GDPR or CCPA, it is agnostic about what a resource owner has to disclose, allowing for resource owners to potentially publish fairly vague descriptions of their resources and data practices, and possibly enriching their entries over time. As such the IoTPI does not take responsibility for ensuring that

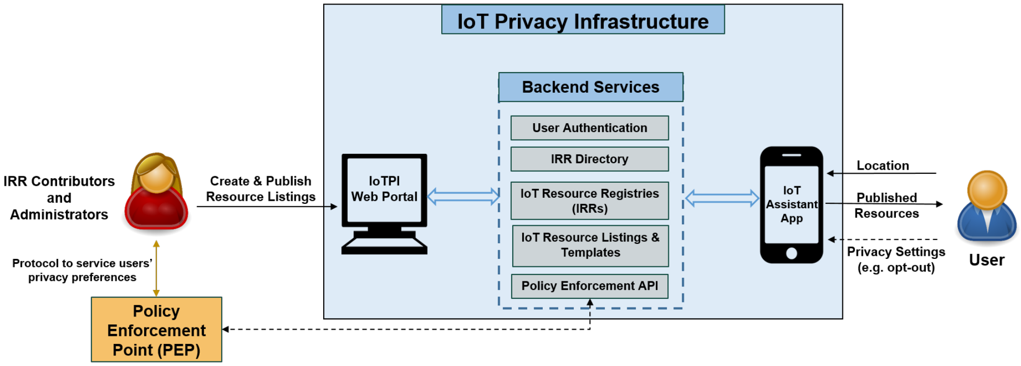
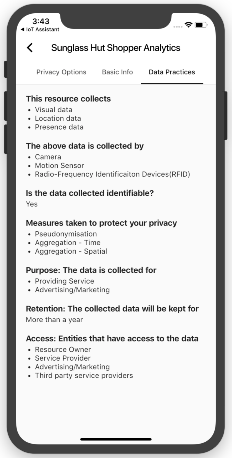

IoT Privacy Infrastructure
Backend Services
User Authentication
IRR Directory
IoT Resource Registries (IRRs)
IoT Resource Listings & Templates
Policy Enforcement API
IoTPI Web Portal
IoT Assistant App
IRR Contributors and Administrators
Create & Publish Resource Listings
Protocol to service users' privacy preferences
Policy Enforcement Point (PEP)
Location
Published Resources
Privacy Settings (e.g. opt-out)
User

Figure 1: High level architecture of the IoT Privacy Infrastructure

IoT resource descriptions are compliant with any particular regulatory requirements. This is left to the resource owners.

IoT resource listings can be discovered by users via an IoT Assistant(IoTA) app they can download on their smartphones. The IoT Assistants also enable users to discover and interact with any available privacy options exposed by a given resource, if such options are available. As shown in Figure 1, the interaction between IoT resource owners/administrators and the public (i.e., data subjects) is facilitated by the IoTPI through several key components, which are further described below:

- **IoT Resource Registries (IRRs)** are repositories managed by individuals or organizations that allow IoT resource owners to publicize the presence of their resources and their data practices. A mall could manage an IRR to help store owners advertise the presence of their IoT resources (e.g. cameras tracking the items that shoppers look at, or tracking functionality used to recognize shoppers and push offers to them). A smart city might have one or more registries enabling people to discover the presence of smart trash cans, smart traffic lights or other IoT systems collecting data about them. An activist could manage a registry to collect information about all surveillance cameras in a given neighborhood. The IoTPI allows people or organizations that manage a given registry to control when a resource description is sufficient to warrant being published. For instance, an IRR administrator might want to ensure that resources collecting sensitive personal data are only published if they provide data subjects with sufficient details and the ability to explicitly opt in. The infrastructure also includes mechanisms and support for policies aimed at ensuring that people who publish resource descriptions do so in a responsible manner. Management of IRRs involves two roles: *IRR Admins* and *IRR contributors*. *IRR Admins* are generally responsible for what IoT resource listings are published in their IRRs



This resource collects
- Visual data
- Location data
- Presence data

The above data is collected by
- Camera
- Motion Sensor
- Radio-Frequency Identificaiton Devices(RFID)

Is the data collected identifiable?
Yes

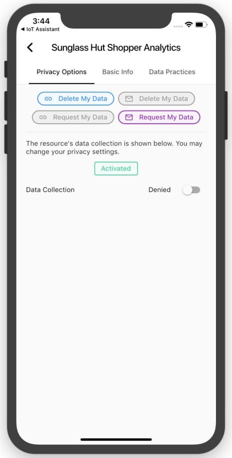
Measures taken to protect your privacy
- Pseudonymisation
- Aggregation - Time
- Aggregation - Spatial

Purpose: The data is collected for
- Providing Service
- Advertising/Marketing

Retention: The collected data will be kept for
More than a year

Access: Entities that have access to the data
- Resource Owner
- Service Provider
- Advertising/Marketing
- Third party service providers

Figure 2: "Data Practices" screen on the IoT Assistant app



The resource's data collection is shown below. You may change your privacy settings.

Data Collection Denied

Figure 3: "Privacy Options" screen on the IoT Assistant app

and may vet publication requests for accuracy and appropriateness.

- **IoT Portal** is the web interface available to all IoT resource owners/administrators (i.e., *IRR contributors*) to create and publish IoT resource listings within relevant IRRs. *IRR Admins* also use this interface to configure their IRRs and manage resource publication.

- **IoT Assistant** is a mobile app which can be used by the public to discover IRRs and IoT resources within their vicinity.

- **Policy Enforcement Points (PEPs)** denote functionality to capture and service privacy choices made by a user for a given IoT resource (e.g. opting in or out of a data practice associated with a given IoT resource, requesting erasure of one's data, request a copy of one's data, etc.). This functionality may be embedded in the IoT resource itself or may be supported by a third party (e.g., third party enforcement point designed to record and control with whom some data collected about a given subject can be shared, or third party enforcement point designed to capture whether a user has opted in for facial recognition functionality (e.g, see [5])

Privacy Management - Notice and Choice

IoTPI aims to facilitate notice and choice in an IoT world by providing usable interfaces for both IoT resource owners/administrators and the general public.

Privacy Notice
IoT Portal users can create IoT resource listings through a step-by-step web form, which utilizes a flexible and detailed taxonomy that captures essential privacy-related data practices assoclayed with a wide range of IoT technologies. IoT Portal users may also utilize IoT resource templates, either created by them or provided by IoT device manufacturers [2]. These templates act as pre-populated resource entries, which can be customized by IoT resource owners.

Privacy Choice
The IoTPI aims to support a wide variety of privacy choices, required under regulations such as GDPR or CCPA, including data deletion, data portability, informed consent as well as any number of opt-ins and opt-outs. IoT resource owners/administrators can configure the privacy options they want to provide to data subjects through PEPs using a web form. We would expect IoT device manufacturers to typically provide this PEP functionality, but also recognize that some IoT devices may be built by individuals or small entities that may lack the resources and know-how to build their own PEP functionality. Accordingly, our IoTPI infrastructure has been designed to also accommodate third party PEP functionality.

Public Release and Future Work

The IoTPI will be made available to the public by the end of the summer. Individuals or organizations interested in managing an IoT Resource Registry (IRR) will be able to submit requests to Carnegie Mellon University to have an IRR set up for them and will be able to start advertising the presence of IoT resources. These IoT resources may be resources they own and control themselves or IoT resources they would like to help others publicize (e.g. mall operator helping store owners publicize the presence and data practices of some of their IoT resources, smart cities, campuses, home owners, etc.) People interested in exploring the use of our infrastructure are invited to contact the authors for additional details.

Acknowledgements

This work is supported in part by the Defense Advanced Research Projects Agency and the Air Force Research Laboratory under agreement number FA8750-15-2-0277 and by the National Science Foundation under grant SBE-1513957.

REFERENCES

1. IoT Analytics. 2018. State of the IoT 2018. `https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/`. (August 2018).

2. Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (2018), 35–46.

3. FTC. 2015. *Internet of Things: Privacy & Security in a Connected World*. Technical Report. Federal Trade Commission (FTC).

4. Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS'2016)*. 27–41.

5. Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. 2018. Enabling Live Video Analytics with a Scalable and Privacy-Aware Framework. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 14, 3s (2018), 64.