Design of a Privacy Infrastructure for the Internet of Things*

Speaker: Norman Sadeh

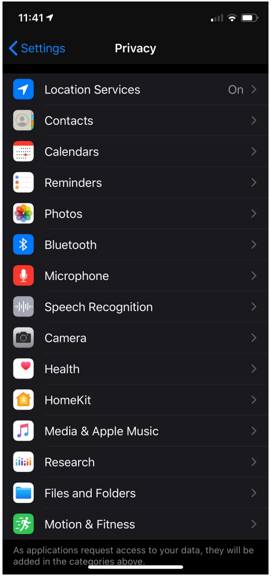
Collaborators: J. Donnell, Y. Feng, Y. Yao, A. Das, M. Degeling, G. Misra, M. Beri, A. Jain, E. Louie, P. Mogali, Y. Torralva, G. Zanfir-Fortuna

Carnegie Mellon University

https://iotprivacy.io

*Patents pending

Smartphone Permission Managers



11:41

Settings

Privacy

Location Services On

Contacts

Calendars

Reminders

Photos

Bluetooth

Microphone

Speech Recognition

Camera

Health

HomeKit

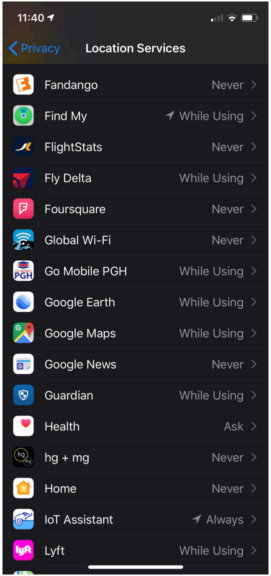
Media & Apple Music

Research

Files and Folders

Motion & Fitness

As applications request access to your data, they will be added in the categories above.



11:40

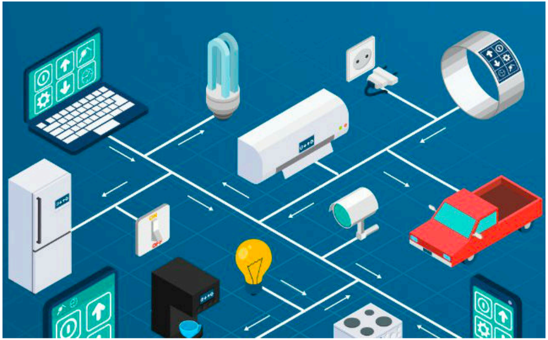
Privacy

Location Services

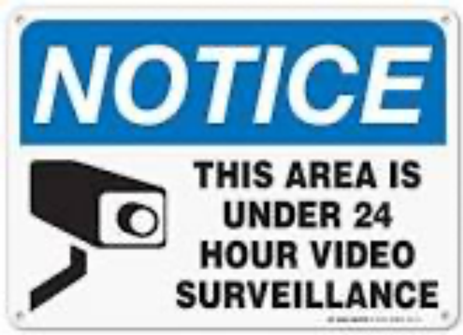
Fandango	Never
Find My	While Using
FlightStats	Never
Fly Delta	While Using
Foursquare	Never
Global Wi-Fi	Never
Go Mobile PGH	While Using
Google Earth	While Using
Google Maps	While Using
Google News	Never
Guardian	While Using
Health	Ask
hg + mg	Never
Home	Never
IoT Assistant	Always
Lyft	While Using

All (or most of) your app privacy settings in one place

But how about with the Internet of Things (IoT)?



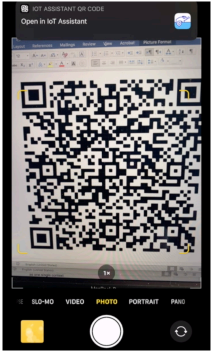
- Where **you don’t control** many of the IoT technologies that collect data about you
- …and are often **not even aware** of their presence

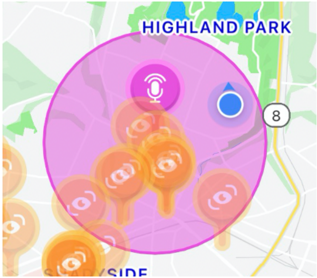


- How likely are you to notice this sign?
- Does this include facial recognition?
- What about facial expression or scene recognition?
- How long is the data retained?
- Do I get to opt in/opt out?
- Is this GDPR or CCPA compliant?

Possible Solutions

- **QR codes**
  - Not always easy to spot; sometimes large area; sometimes area is too crowded
- **Location-based discovery**
  - More flexible, but could be missed too unless combined with notifications
- **…How about supporting both?**





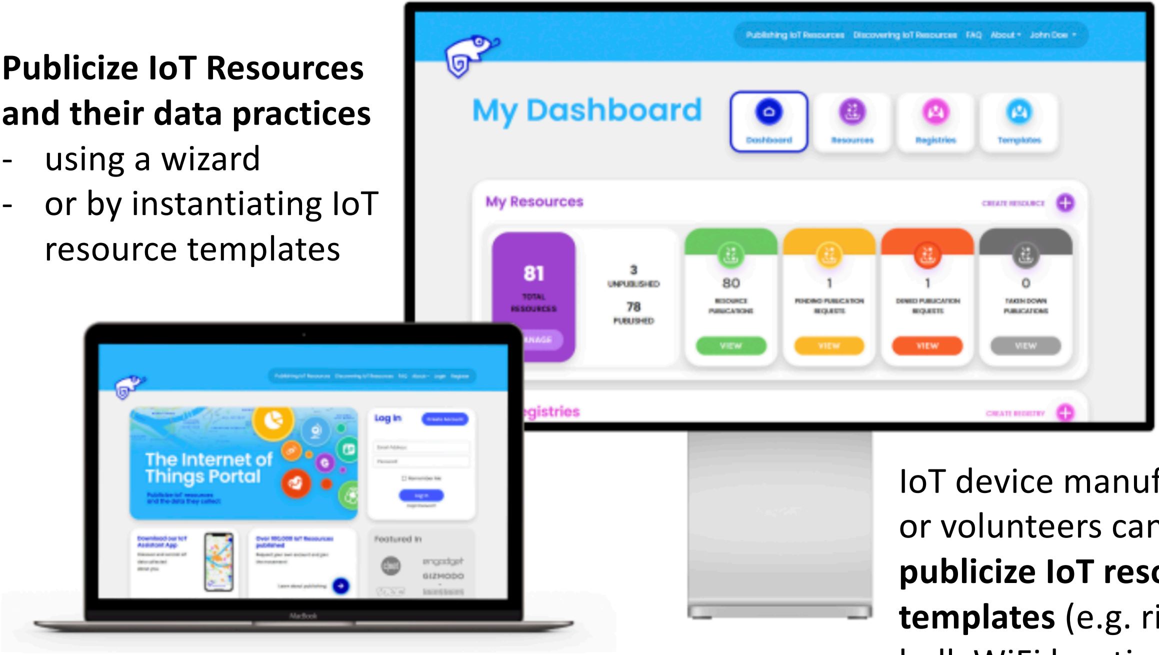
Why an IoT Privacy Infrastructure?

Offer **unified platform/UIs** to:

1. **Publicize IoT resources collecting data, incl. privacy options** (e.g., opt-in/out, deletion, portability)
   - **IoT Portal** for resource owners, device manufacturers, and volunteer contributors
2. **Discover nearby IoT resources, incl. privacy options**
   - Privacy Assistant mobile app to help data subjects

Publicize IoT Resources and their data practices

- using a wizard
- or by instantiating IoT resource templates

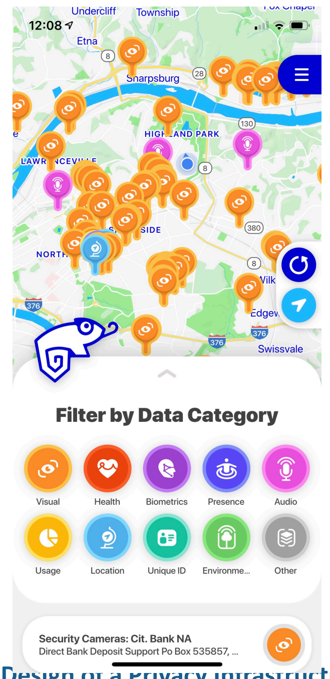


IoT device manufacturers or volunteers can also **publicize IoT resource templates** (e.g. ring door bell, WiFi location tracking, etc.)

Publicizing IoT Data Collection

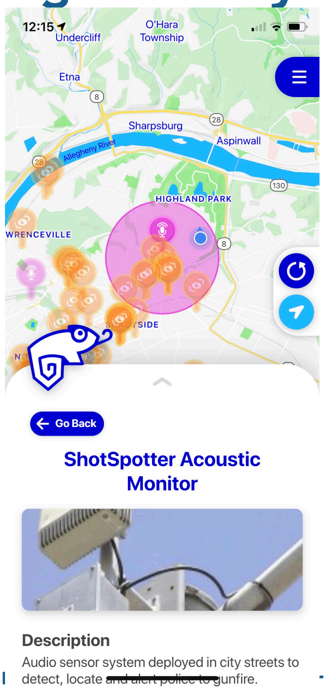
- **IoT resource owner:** Publicize your IoT resources & data practices
- **IoT volunteer contributor:** Report IoT resources & assumed data practices
- **IoT registry owner:** Aggregate and curate IoT resource publication (e.g. building, neighborhood, mall, etc.)
- **IoT device manufacturer/service provider:** Publicize IoT resource templates

Discovering Nearby IoT Data Collection



Filter by Data Category

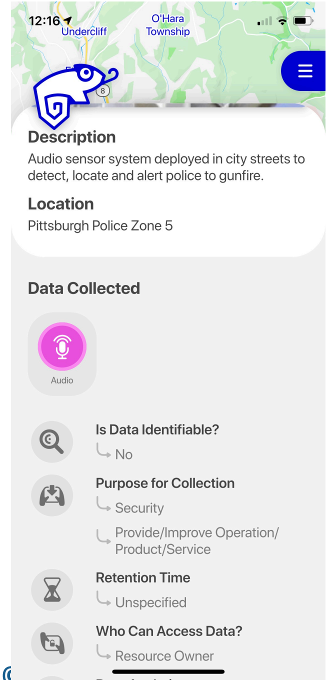
Security Cameras: Cit. Bank NA
Direct Bank Deposit Support Po Box 535857, ...



ShotSpotter Acoustic Monitor

Description

Audio sensor system deployed in city streets to detect, locate and alert police to gunfire.



Description

Audio sensor system deployed in city streets to detect, locate and alert police to gunfire.

Location

Pittsburgh Police Zone 5

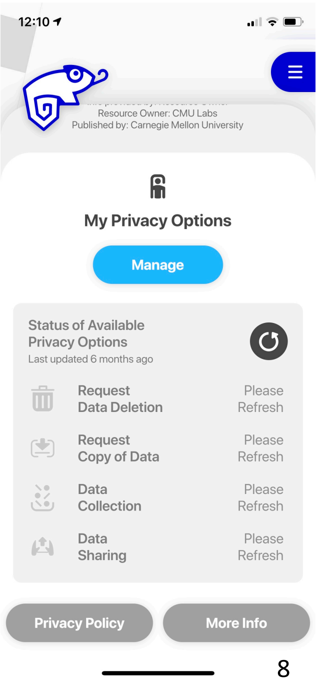
Data Collected

Is Data Identifiable?
No

Purpose for Collection
Security
Provide/Improve Operation/Product/Service

Retention Time
Unspecified

Who Can Access Data?
Resource Owner



Resource Owner: CMU Labs
Published by: Carnegie Mellon University

My Privacy Options

Status of Available Privacy Options
Last updated 6 months ago

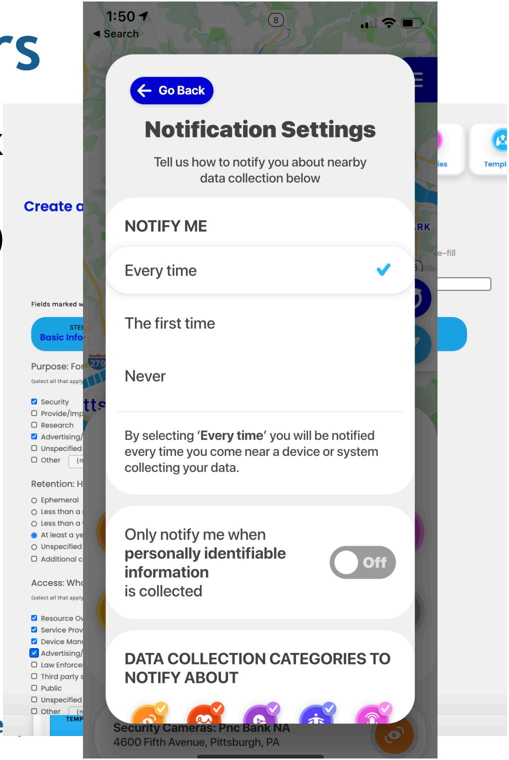
Request Data Deletion	Please Refresh
Request Copy of Data	Please Refresh
Data Collection	Please Refresh
Data Sharing	Please Refresh

Design Challenges (Short Selection)

- Should be usable by **lay users** – occasionally some privacy professionals
- Should be **jurisdiction-agnostic**
  - Capable of supporting GDPR or CCPA without requiring it
- Supporting **data subject rights** without actually managing those rights
- Discourage **abuse**

Usable by Lay Users

- **Device templates** (e.g. ring door bell, Alex smart speaker, but also video analytics in a mall or WiFi location tracking on a campus)
- Encourage both **resource owners & volunteer contributors** to publish
- **Wizard with drop-down menus** to assist users when describing one-off resources
- Intuitive mobile app supporting both **location-based discovery and QR codes**
  - **Customizable notifications**



Purpose: For
(select all that apply)
☑ Security
□ Provide/Imp
□ Research
☑ Advertising/
□ Unspecified
□ Other

Retention: H
○ Ephemeral
○ Less than a
○ Less than a
● At least a ye
○ Unspecified
□ Additional c

Access: Who
(select all that apply)
☑ Resource Ow
☑ Service Prov
☑ Device Manu
☑ Advertising/
□ Law Enforce
□ Third party s
□ Public
□ Unspecified
□ Other

Notification Settings

Tell us how to notify you about nearby data collection below

NOTIFY ME

Every time ✓

The first time

Never

By selecting **'Every time'** you will be notified every time you come near a device or system collecting your data.

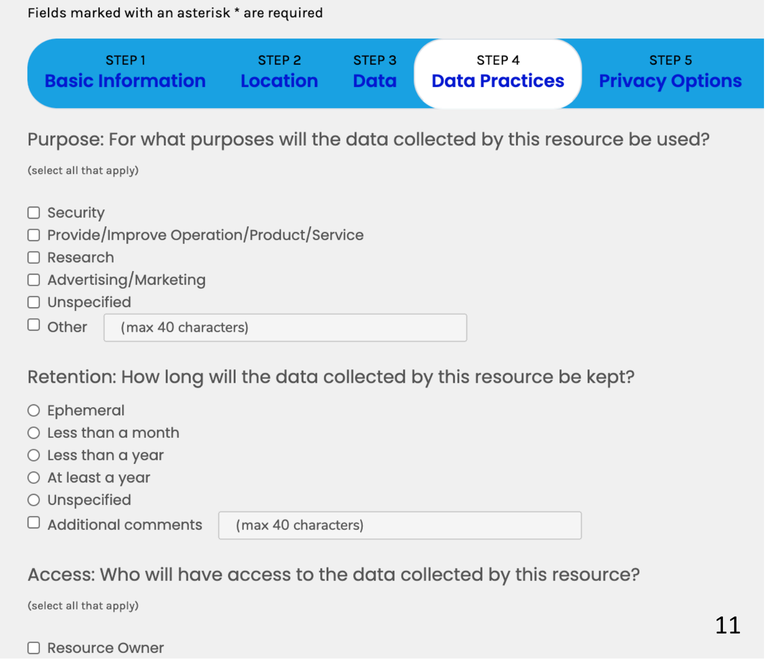
Only notify me when **personally identifiable information** is collected — Off

DATA COLLECTION CATEGORIES TO NOTIFY ABOUT

Security Cameras: Pnc Bank NA
4600 Fifth Avenue, Pittsburgh, PA

Jurisdiction-Agnostic (I)

- Rich set of options to capture diverse disclosure requirements
- Required fields kept to a minimum



Fields marked with an asterisk * are required

Purpose: For what purposes will the data collected by this resource be used?

(select all that apply)

□ Security
□ Provide/Improve Operation/Product/Service
□ Research
□ Advertising/Marketing
□ Unspecified
□ Other (max 40 characters)

Retention: How long will the data collected by this resource be kept?

○ Ephemeral
○ Less than a month
○ Less than a year
○ At least a year
○ Unspecified
□ Additional comments (max 40 characters)

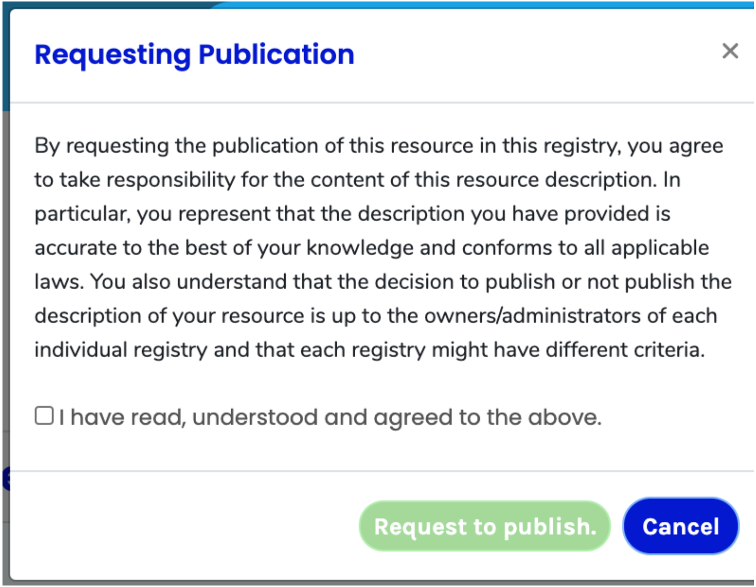
Access: Who will have access to the data collected by this resource?

(select all that apply)

□ Resource Owner

Jurisdiction-Agnostic (II)

- …but make people accountable



Requesting Publication

By requesting the publication of this resource in this registry, you agree to take responsibility for the content of this resource description. In particular, you represent that the description you have provided is accurate to the best of your knowledge and conforms to all applicable laws. You also understand that the decision to publish or not publish the description of your resource is up to the owners/administrators of each individual registry and that each registry might have different criteria.

□ I have read, understood and agreed to the above.

Support Data Subject Rights without Managing Those Rights

- **Support open collection of privacy options** (e.g., opt-in/out for different practices, deletion, portability, etc.)
- **Open APIs to connect to different consent management platforms**
- Support 3rd **party authentication** to capture user selection of privacy options
  - And relevant identifying data, if needed.

Discouraging Abuse

- All users are **authenticated**
  - Allow for **volunteer contributors**…but require contributors to **take responsibility** for what they publish
- **Decentralized publication mechanism** managed via **registries** (e.g., mall operator, campus, home owner, neighborhood association)
- Each **registry owner reviews** publication requests and has the option to reject requests or take down publications
- Platform can take down any registry or resource - whether temporarily or permanently

Current Status

- **Initial release**: 17,000 mobile app downloads within a week
  - approaching 200,000 IoT resources today

- **Improved portal and IoT Assistant app to be released in October 2020…**
- **Stay tuned!**
  - https://iotprivacy.io

  -Consider also subscribing to **our mailing list at:** https://www.privacyassistant.org/contact/

THANK YOU!

- **IoT Portal:** https://iotprivacy.io
- **IoT Assistant app** available in Google Play Store and iOS iTunes store.

Download on the App Store

GET IT ON Google Play

- Work funded by the **National Science Foundation** under the Secure and Trustworthy Computing initiative and under the **DARPA/AFRL Brandeis privacy research initiative**. Additional funding provided by **CyLab** and **Google -** https://www.privacyassistant.org/

A. Das, M. Degeling, D. Smullen, and N. Sadeh, "Personalized Privacy Assistants for the Internet of Things", 2018 IEEE Pervasive Computing: Special Issue - Securing the IoT, Apr 2018