Assisting Users in a World Full of Cameras

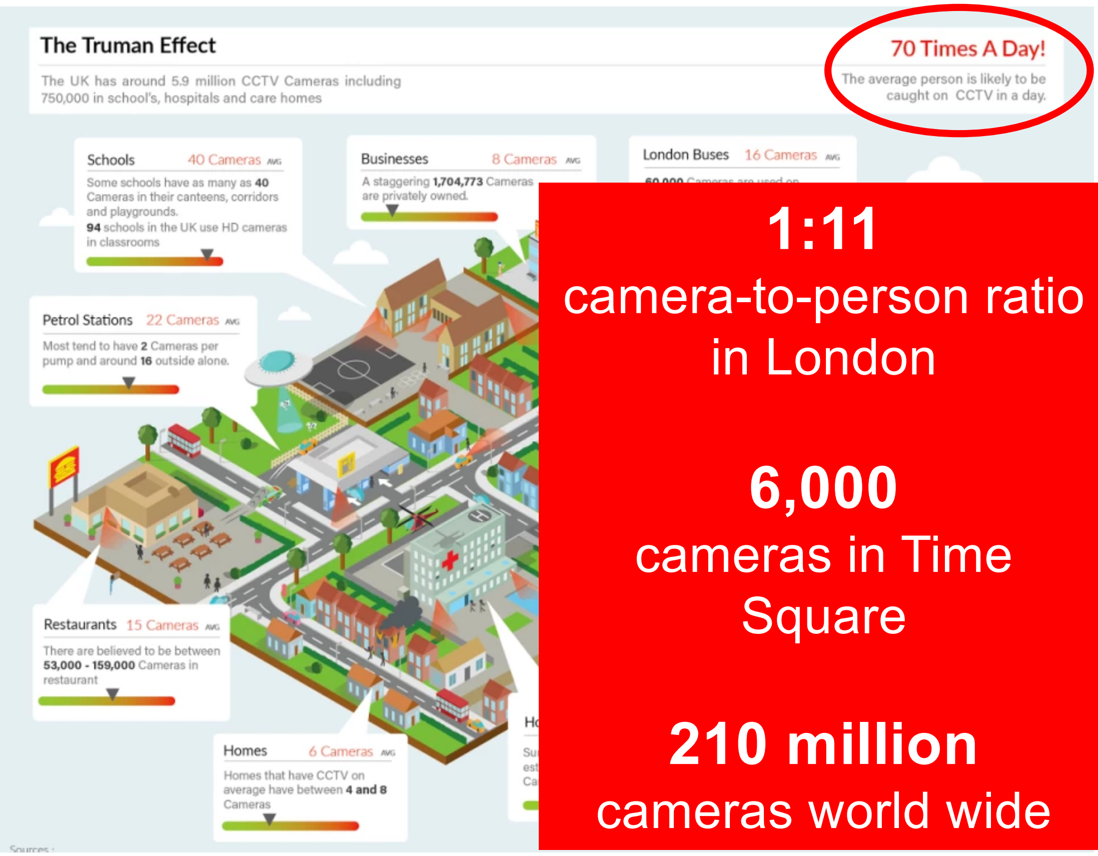
Privacy-Aware Infrastructure for Computer Vision Applications

CV-COPS 2017

Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang,
Norman Sadeh, Mahadev Satyanarayanan

Carnegie
Mellon
University

Cameras are Everywhere



The Truman Effect

The UK has around 5.9 million CCTV Cameras including 750,000 in school's, hospitals and care homes

70 Times A Day!

The average person is likely to be caught on CCTV in a day.

Schools 40 Cameras AVG

Some schools have as many as **40** Cameras in their canteens, corridors and playgrounds.
94 schools in the UK use HD cameras in classrooms

Businesses 8 Cameras AVG

A staggering **1,704,773** Cameras are privately owned.

London Buses 16 Cameras AVG

Petrol Stations 22 Cameras AVG

Most tend to have **2** Cameras per pump and around **16** outside alone.

Restaurants 15 Cameras AVG

There are believed to be between **53,000 - 159,000** Cameras in restaurant

Homes 6 Cameras AVG

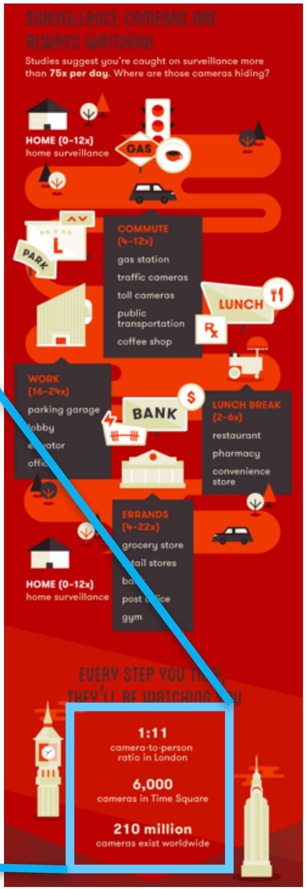
Homes that have CCTV on average have between **4 and 8** Cameras

1:11
camera-to-person ratio in London

6,000
cameras in Time Square

210 million
cameras world wide

Sources: Association of Chief Police Officers, CCTV User Group, The Guardian, Channel 4 news, The Telegraph



SURVEILLANCE CAMERAS ARE ALWAYS WATCHING

Studies suggest you're caught on surveillance more than **75x per day**. Where are those cameras hiding?

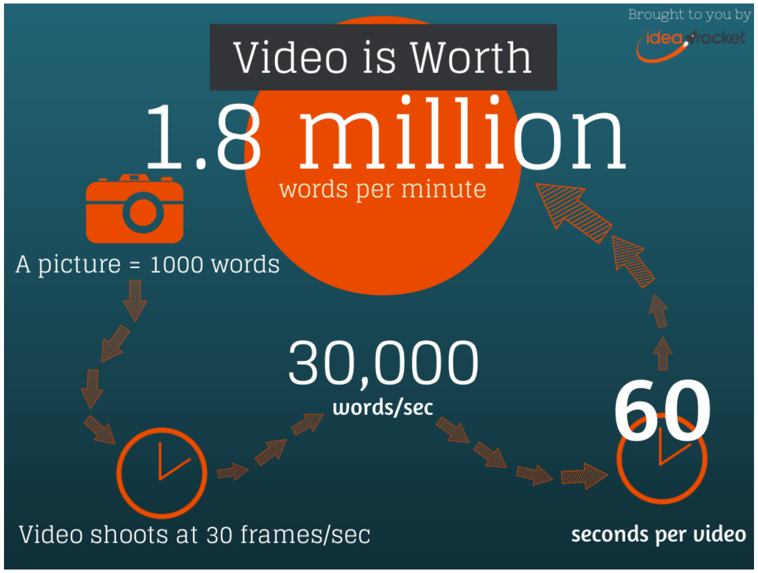
Source: UrbanEye, New York Civil Liberty Union

More Gadgets with Cameras

A Picture is Worth 1000 Words

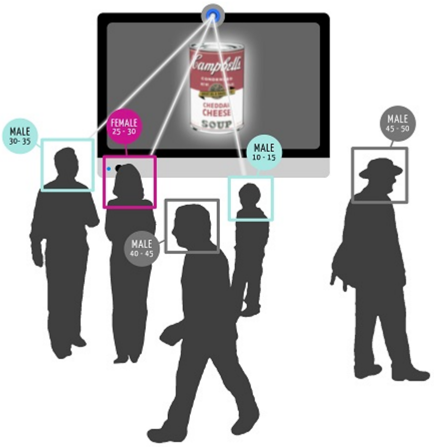
Images can be used for:

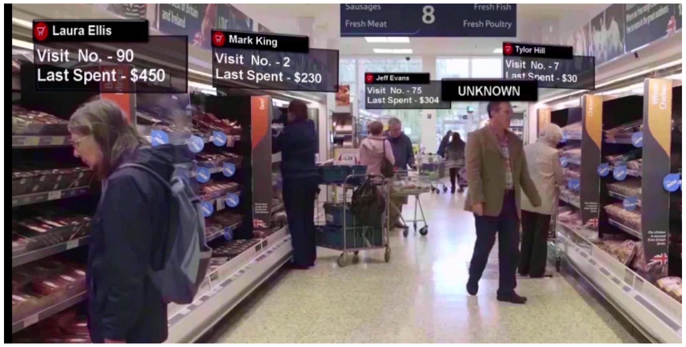
- Facial recognition
  - Identification
  - Mood / Expression / Health
  - Demographics
- Object recognition
- Scene recognition
- Activity recognition
- Safety and security
  - surveillance, criminal investigation



Source: IdeaRocket

Use of Facial Recognition is on the Rise





To verify your identity please look into the camera
We are performing a match only. Your biometric data will NOT be stored
11 lbs
DELTA

Privacy Implications of Facial Recognition

Facial Recognition can be used to:

- Generate a customer/user profile
  - Serve customized ads/services
- Infer lifestyle, behavior, and habits
- Infer health conditions
- Track users' whereabouts
- Infer social associations and activities

Regulators and policymakers advocate the right to **notice** and **choice**.

Privacy Preference Study

Vignette Study on IoT privacy preferences:

- 1007 Amazon MTurk participants gave feedback for 380 scenarios consisting of eight factors.
- Each user saw at least one scenario involving facial recognition.

Example Scenario:

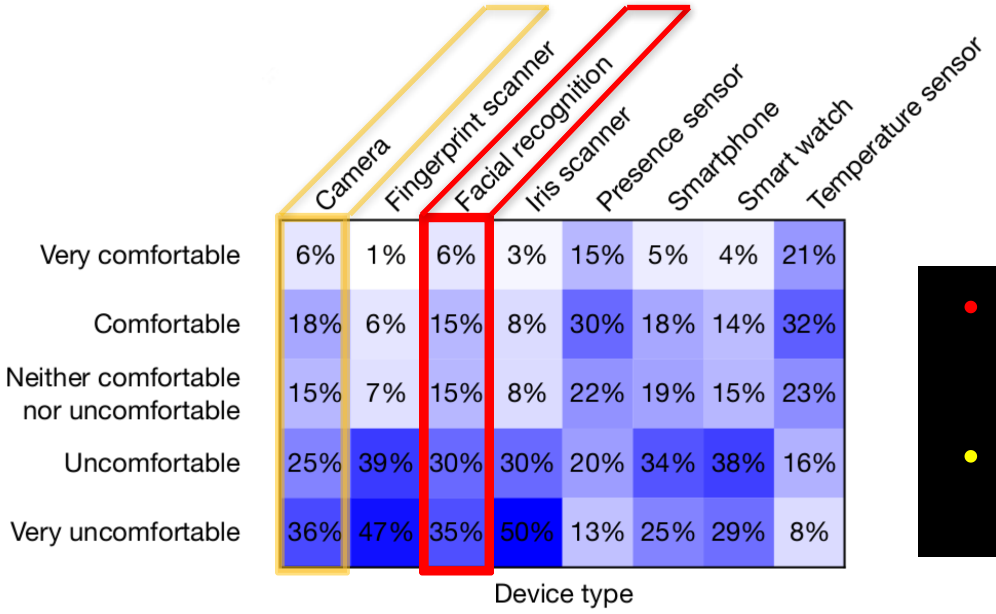
"You are at a [coffee shop]. This store uses [facial recognition system] to automatically [identify returning customers]. The system is also used to keep track of [your orders and make suggestions] based on your ordering habits. Your picture will be kept for [a few hours]".

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

https://www.privacyassistant.org/publications

Users are Uncomfortable with Image Data

- Self-reported comfort level for different data collection devices (regardless of the specific scenario)



	Camera	Fingerprint scanner	Facial recognition	Iris scanner	Presence sensor	Smartphone	Smart watch	Temperature sensor
Very comfortable	6%	1%	6%	3%	15%	5%	4%	21%
Comfortable	18%	6%	15%	8%	30%	18%	14%	32%
Neither comfortable nor uncomfortable	15%	7%	15%	8%	22%	19%	15%	23%
Uncomfortable	25%	39%	30%	30%	20%	34%	38%	16%
Very uncomfortable	36%	47%	35%	50%	13%	25%	29%	8%

Device type

- **65%** of the users were uncomfortable with **facial recognition**
- **61%** of the users were uncomfortable with **data captured by cameras**

Users Want Notice and Choice

- Users expressed interest in being **notified** about the presence of facial recognition especially when the data collection purpose is unclear.

- Most would **disable** facial recognition if given the option.

- **Context** has an impact on the decision.
  - More likely to allow in a library than in a department store.

Our Goals

- Support **notice and choice** in IoT.
- **Objective:** Selectively notify users without overwhelming them and help them configure available settings.
  - **Capture users' privacy preferences:**
    - Notification preferences (when, how often, how)
    - Data collection and sharing preferences

Building a Privacy-Aware Infrastructure

Internet of Things Resource Registry (IRR)

- Advertises privacy practices (including any privacy settings) and capabilities of IoT resources (e.g., apps, sensors, services)
- Multiple registries controlled by different entities

Personalized Privacy Assistants (IoT Assistant)

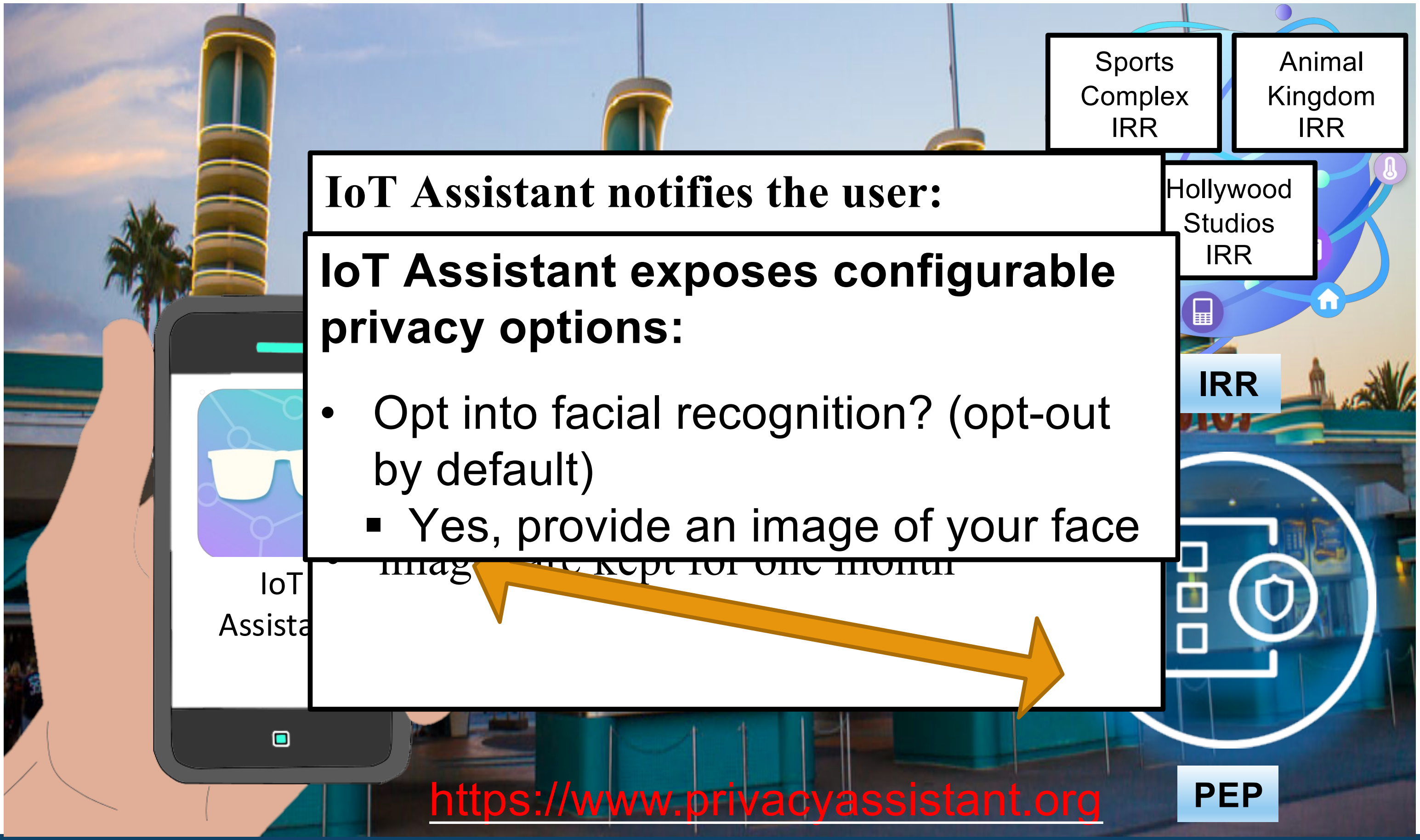
- Discovers IoT resources, their capabilities, and privacy practices (including any privacy settings)
- Learns user preferences; supports selective user notification, and semi-automated configuration of settings

Policy Enforcement Point (PEP)

- Captures and stores user-specific privacy settings (e.g., opt in/out)
- Enforces users' privacy settings

https://www.privacyassistant.org

Workflow Example: Theme Park



IoT Assistant notifies the user:

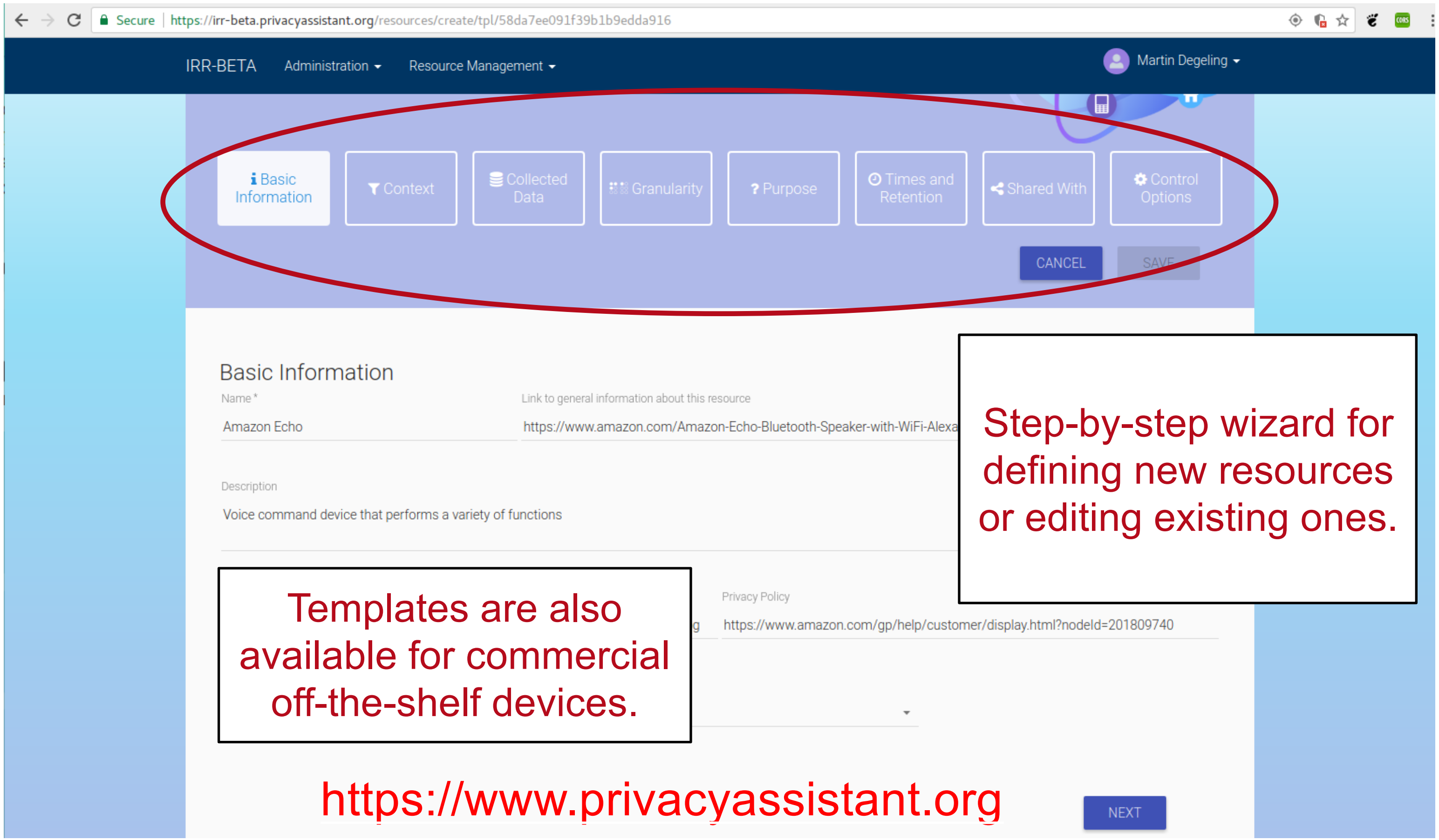
- images are kept for one month

IoT Assistant exposes configurable privacy options:

- Opt into facial recognition? (opt-out by default)
  - Yes, provide an image of your face

https://www.privacyassistant.org

Registering an IRR Resource



Basic Information

Name *
Amazon Echo

Link to general information about this resource
https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa

Description
Voice command device that performs a variety of functions

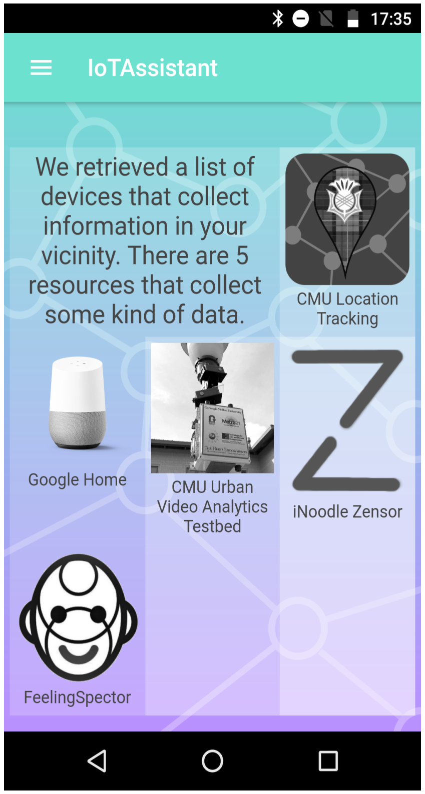
Privacy Policy
https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740

Step-by-step wizard for defining new resources or editing existing ones.

Templates are also available for commercial off-the-shelf devices.

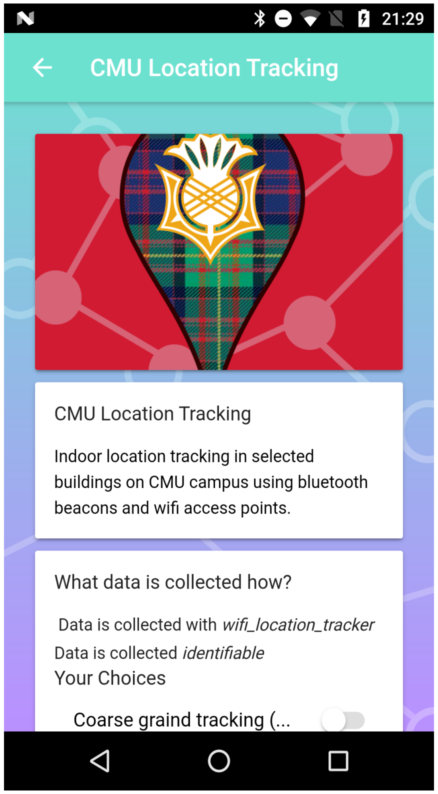
https://www.privacyassistant.org

IoT Assistant Discovering IRR Resources



IoTAssistant

We retrieved a list of devices that collect information in your vicinity. There are 5 resources that collect some kind of data.



CMU Location Tracking

CMU Location Tracking

Indoor location tracking in selected buildings on CMU campus using bluetooth beacons and wifi access points.

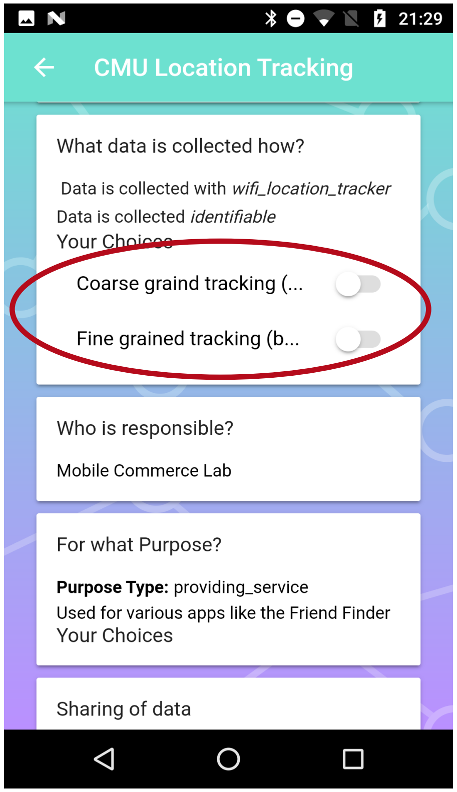
What data is collected how?

Data is collected with *wifi_location_tracker*

Data is collected *identifiable*

Your Choices

Coarse graind tracking (...



CMU Location Tracking

What data is collected how?

Data is collected with *wifi_location_tracker*

Data is collected *identifiable*

Your Choices

Coarse graind tracking (...

Fine grained tracking (b...

Who is responsible?

Mobile Commerce Lab

For what Purpose?

Purpose Type: providing_service

Used for various apps like the Friend Finder

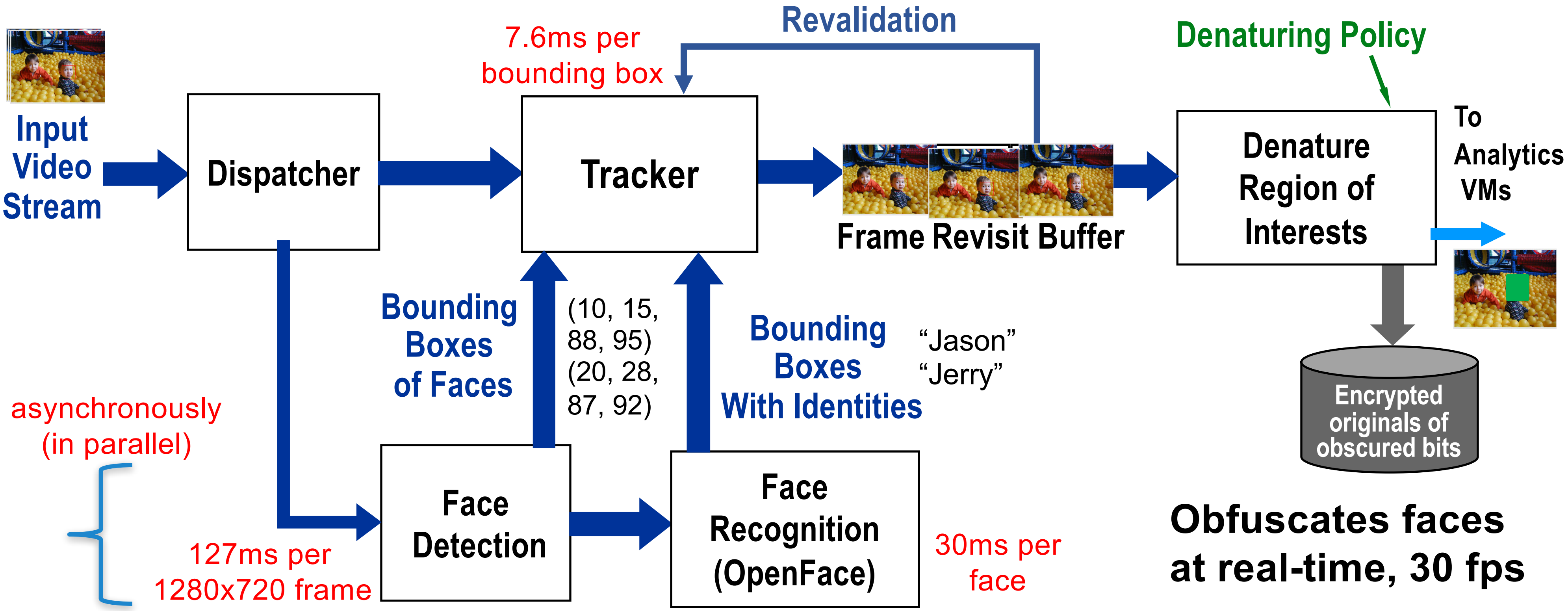
Your Choices

Sharing of data

Exposes privacy settings.

https://www.privacyassistant.org

Privacy-Aware Video Streaming



Input Video Stream

Dispatcher

7.6ms per bounding box

Tracker

Revalidation

Frame Revisit Buffer

Denaturing Policy

Denature Region of Interests

To Analytics VMs

Encrypted originals of obscured bits

Bounding Boxes of Faces

(10, 15, 88, 95) (20, 28, 87, 92)

Bounding Boxes With Identities

“Jason” “Jerry”

asynchronously (in parallel)

127ms per 1280x720 frame

Face Detection

Face Recognition (OpenFace)

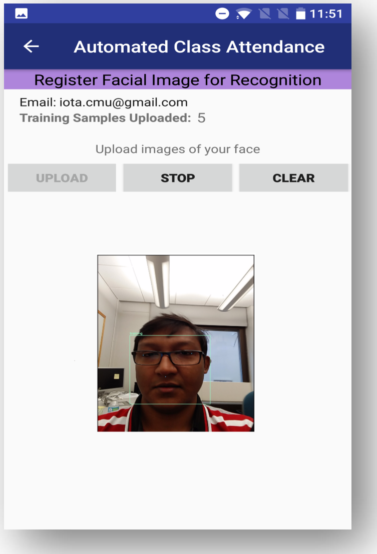
30ms per face

Obfuscates faces at real-time, 30 fps

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 (**Best Paper Award**)

Automated Attendance Tracker

Train Facial Features



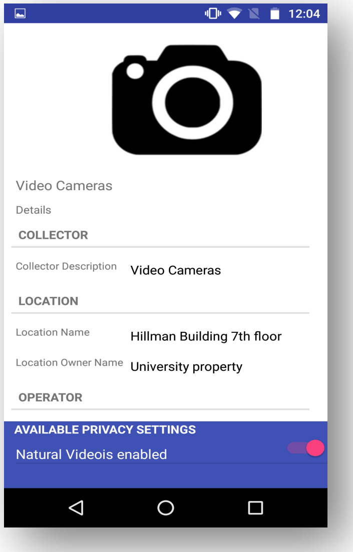
Automated Class Attendance

Register Facial Image for Recognition

Email: iota.cmu@gmail.com
Training Samples Uploaded: 5

Upload images of your face

Control Opt-in



Video Cameras

Details

COLLECTOR

Collector Description: Video Cameras

LOCATION

Location Name: Hillman Building 7th floor

Location Owner Name: University property

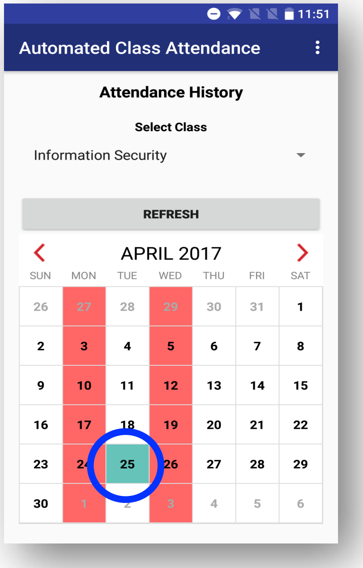
OPERATOR

AVAILABLE PRIVACY SETTINGS

Natural Videois enabled

Live Video Stream

Monitor Class Attendance



Automated Class Attendance

Attendance History

Select Class

Information Security

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	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

- Planning to pilot this system in classrooms at CMU.

Conclusion

- The use of computer vision is expanding with the rise of IoT cameras.
- Our studies show that:
  - Users want to be **notified** about how their data is being used
  - Users want to **choose** (control) how their data is being used
- We are working on an **infrastructure** that supports **notice and choice**, and captures users' **privacy preferences** in IoT settings.

For more information:

https://www.privacyassistant.org

Contact:

anupamd@cs.cmu.edu
sadeh@cs.cmu.edu

Demonstration

https://goo.gl/gtpbpK

This material is based upon work supported in part by the National Science Foundation under grant CNS-1518865, and SBE-1513957, as well as by DARPA and the Air Force Research Laboratory, under agreement number FA8750-15-2-0277. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes not withstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA, the Air Force Research Laboratory, the National Science Foundation, or the U.S. Government.