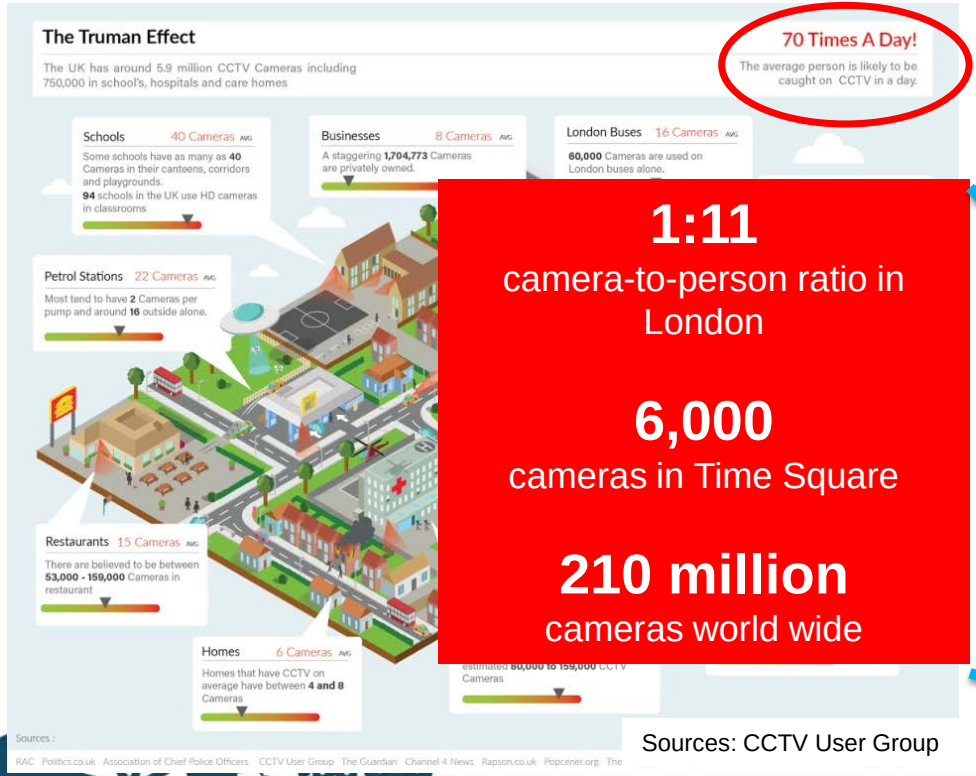
Assisting Users in a World Full of Cameras

Privacy-Aware Infrastructure for Computer Vision Applications

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

PRIVACYCON

Cameras Are Everywhere



1:11
camera-to-person ratio in London

6,000
cameras in Time Square

210 million
cameras world wide

Sources: CCTV User Group

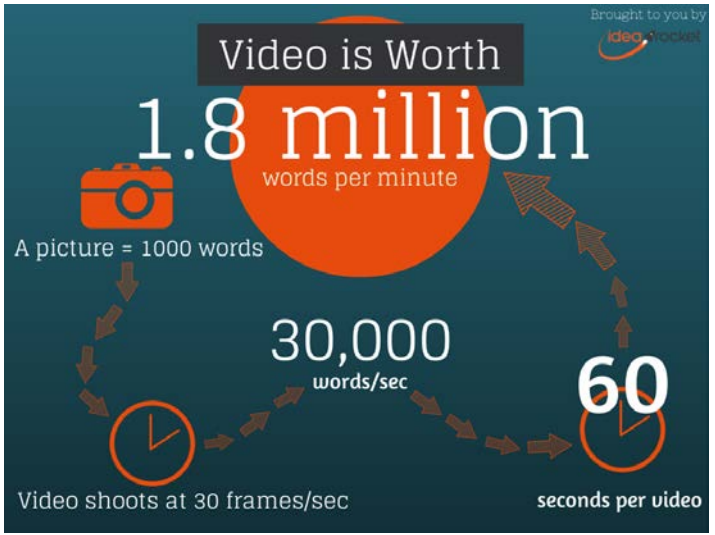
Source: UrbanEye, New York Civil Liberty Union

More Gadgets with Cameras

PRIVACYCON

A Picture Is Worth 1000 Words

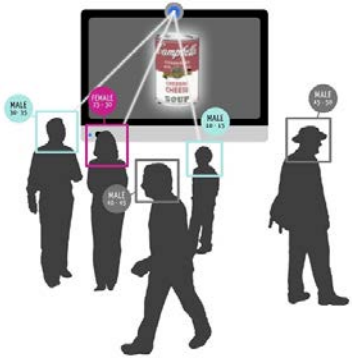
- Facial recognition
  - Identification
  - Mood / Expression / Health
  - Demographics
- Object recognition
- Scene recognition
- Activity recognition
- Safety and security
  - surveillance, criminal investigation



Source: IdeaRocket

Use of Facial Recognition Is on the Rise

Moments



PRIVACYCON

Privacy Implications of Facial Recognition

- 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:

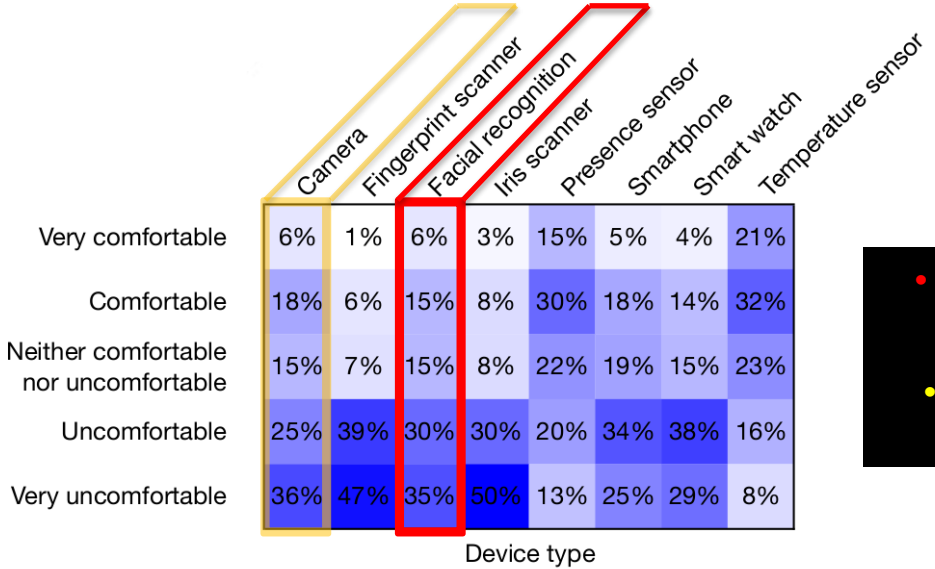
"You are at a [coffee shop]. This store uses [facial recognition system] to automatically [identify returning customers]. The system is also used to keep track of [your orders and make suggestions] based on your ordering habits. Your picture will be kept for [a few hours]".

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)



- **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)

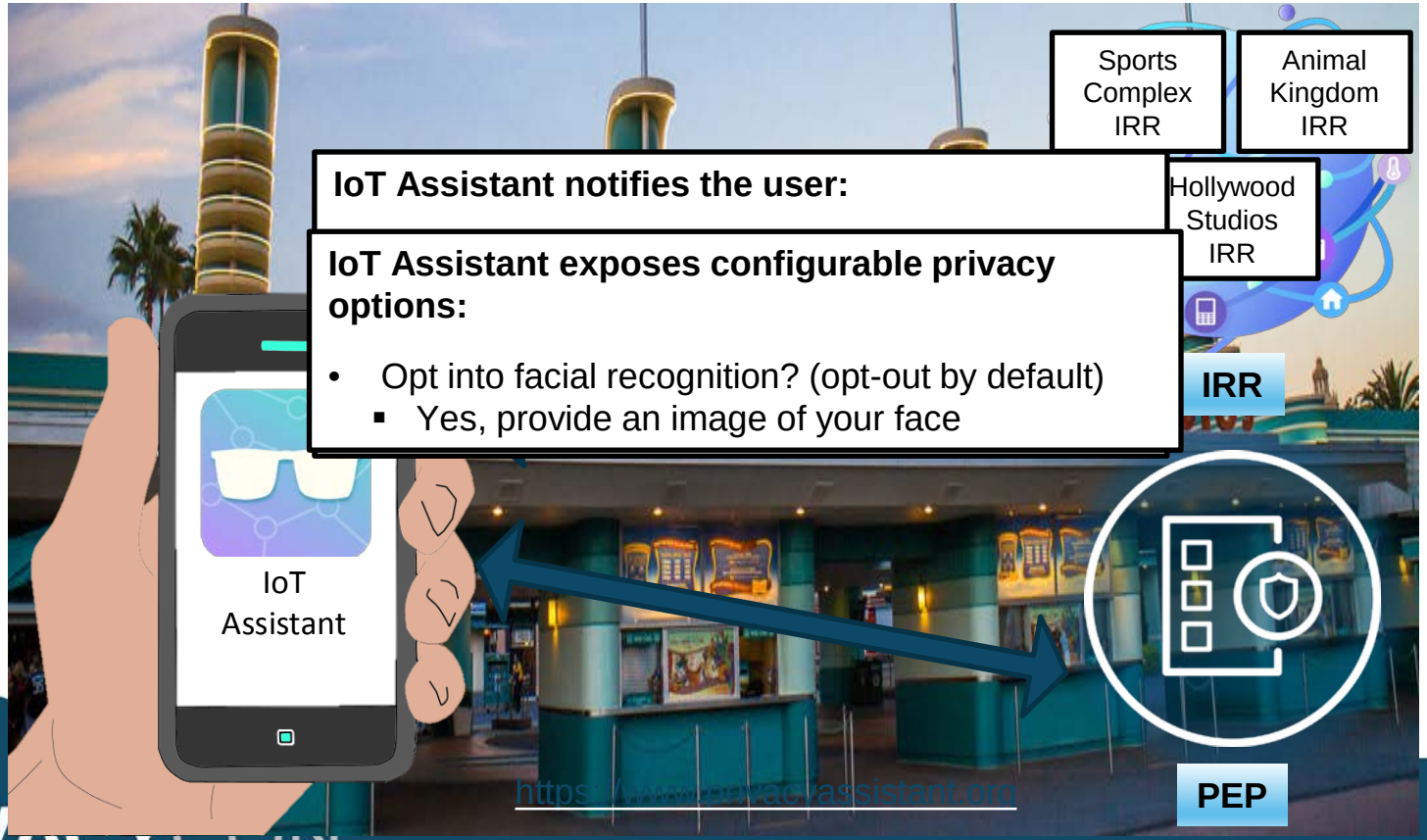
- Discovers IoT resources, their capabilities, and privacy practices (including any privacy settings)
- Learns user preferences; supports selective user notification, and semi-automated configuration of settings

Policy Enforcement Point (PEP)

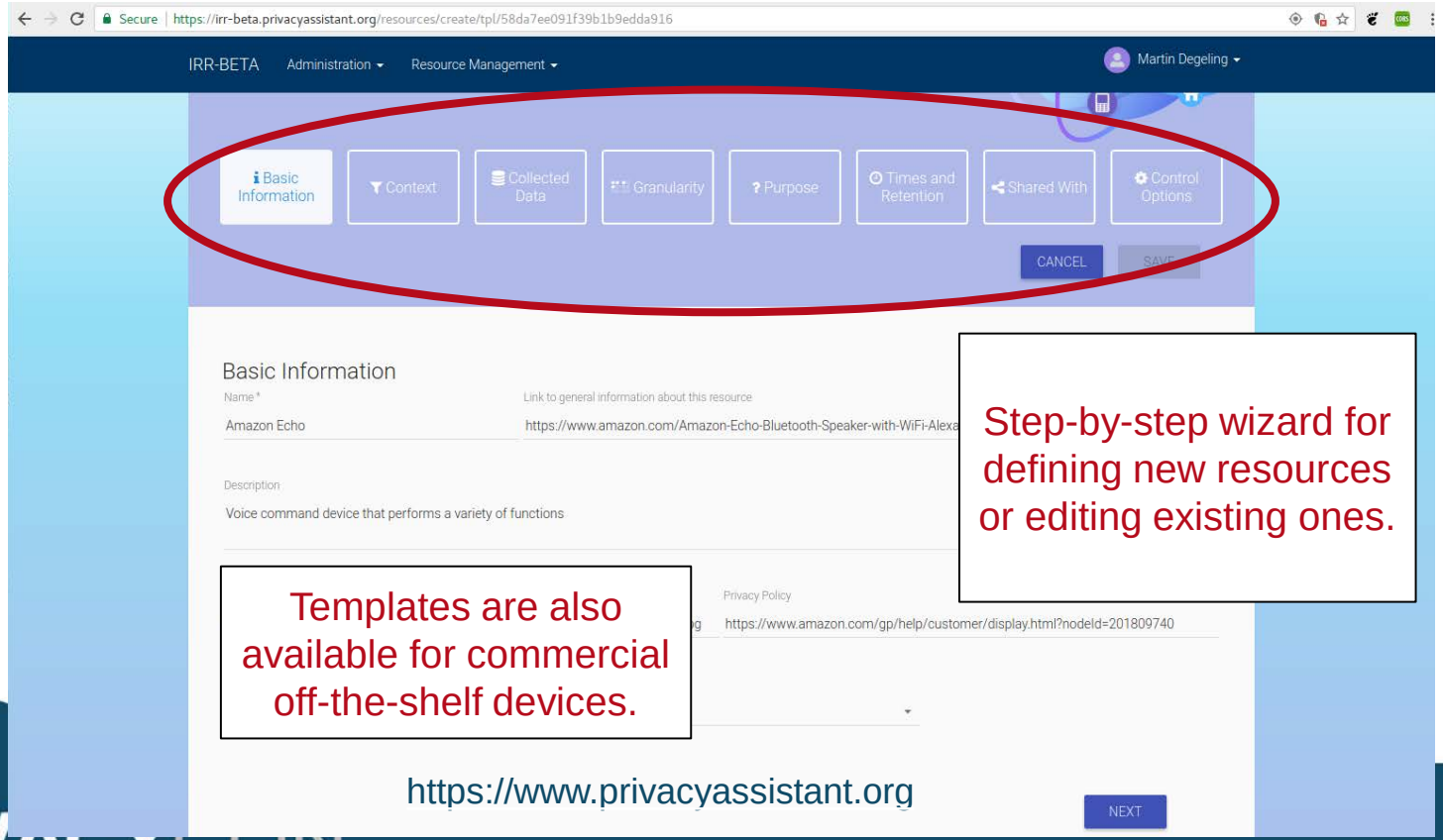
- Captures and stores user-specific privacy settings (e.g., opt in/out)
- Enforces users' privacy settings

https://www.privacyassistant.org

Workflow Example: Theme Park



Registering an IRR Resource

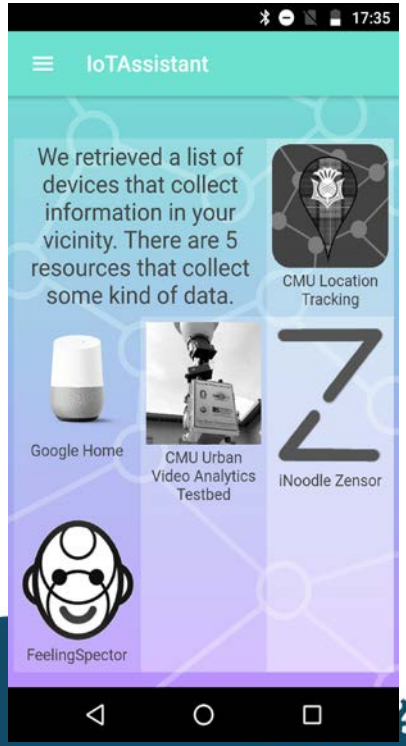


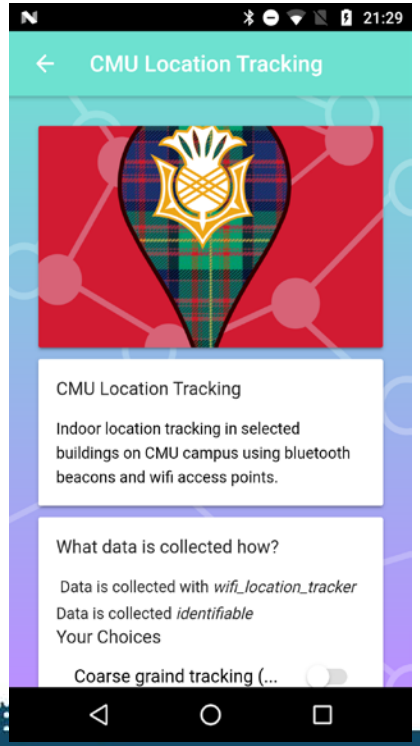
Step-by-step wizard for defining new resources or editing existing ones.

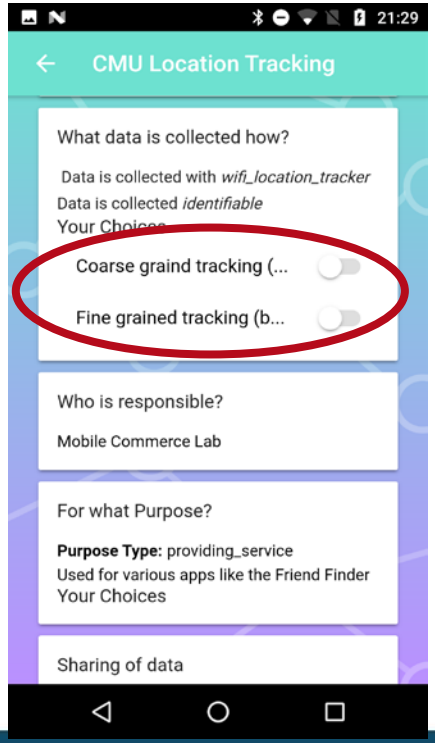
Templates are also available for commercial off-the-shelf devices.

https://www.privacyassistant.org

IoT Assistant Discovering IRR Resources



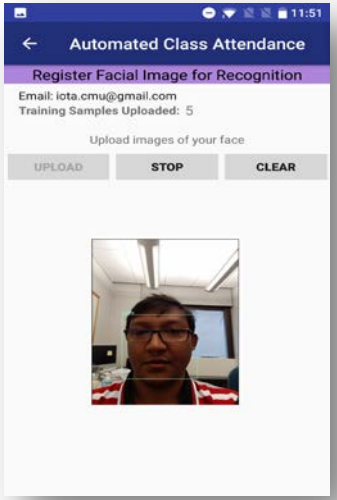




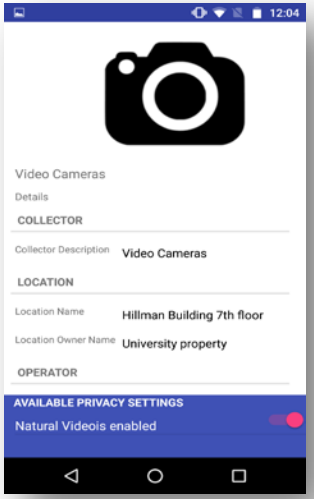
Exposes privacy settings.

Automated Attendance Tracker

Train Facial Features

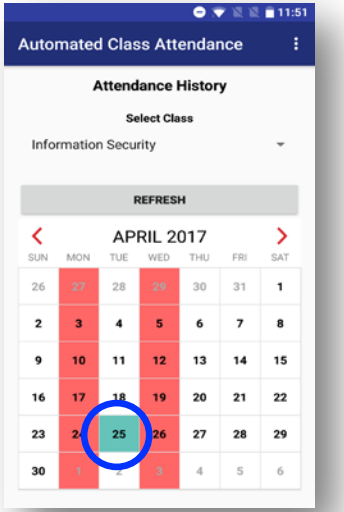


Control Opt-in



Live Video Stream

Monitor Class Attendance



- 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

Demonstration

https://goo.gl/gtpbpK

Contact:

sadeh@cs.cmu.edu

anupamd@cs.cmu.edu

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.