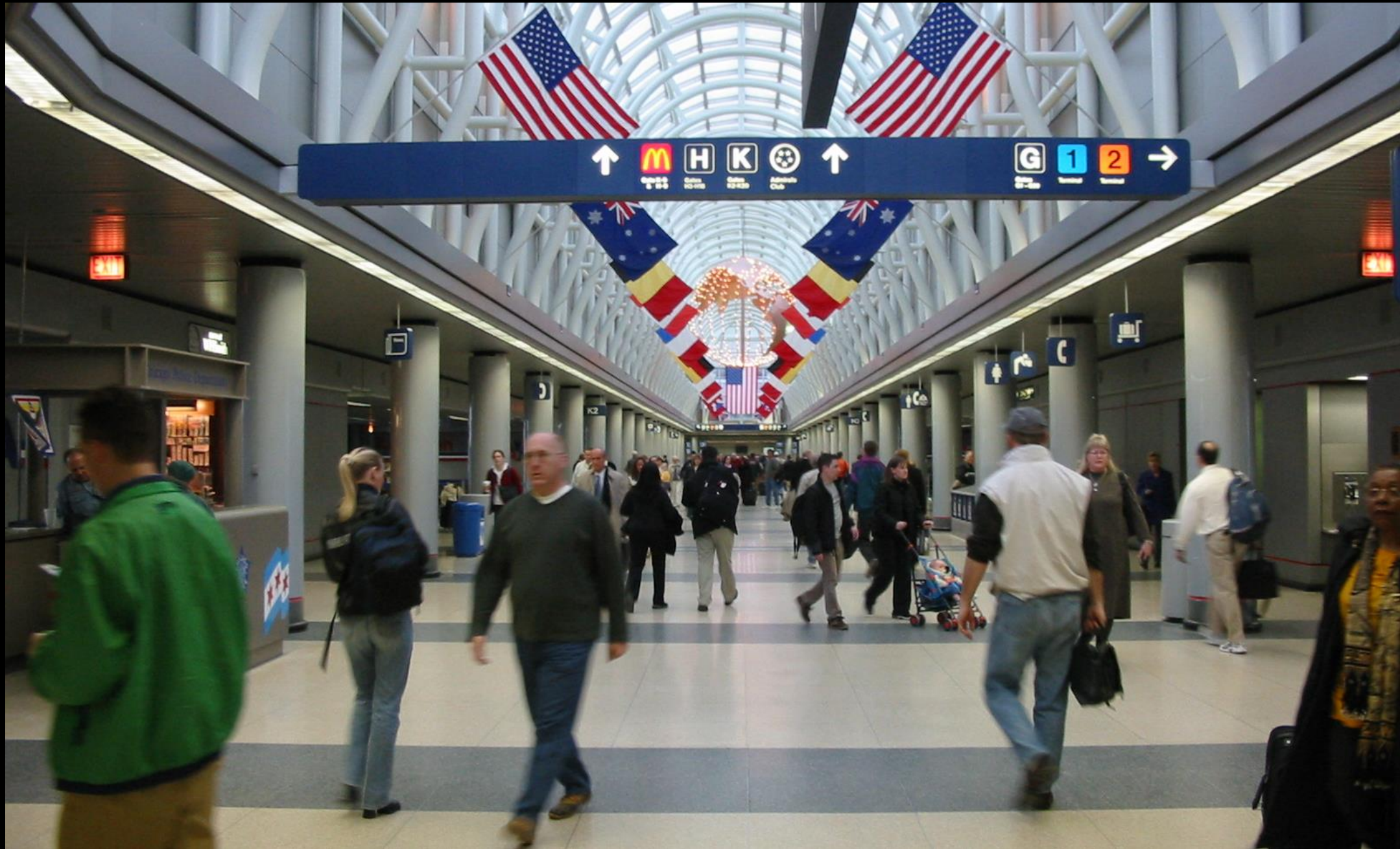


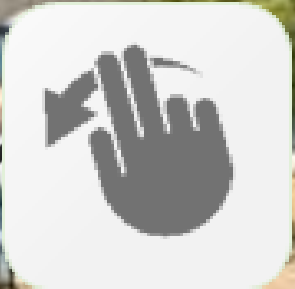
# IoT Privacy: Can We Regain Control?

Foundations of Privacy  
Sept 30, 2015  
CMU

Richard Chow  
Intel Corporation  
[richard.chow@intel.com](mailto:richard.chow@intel.com)





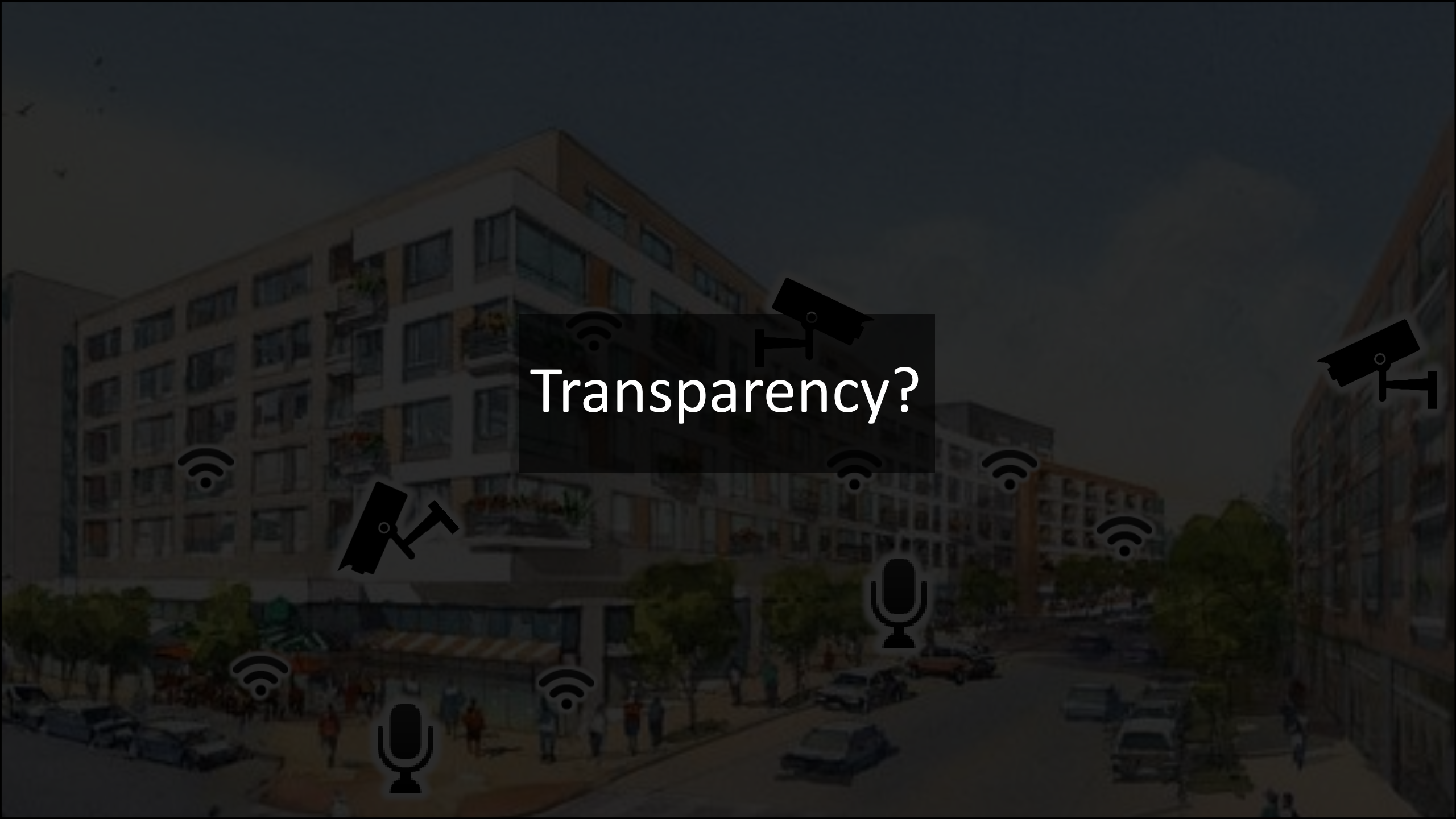






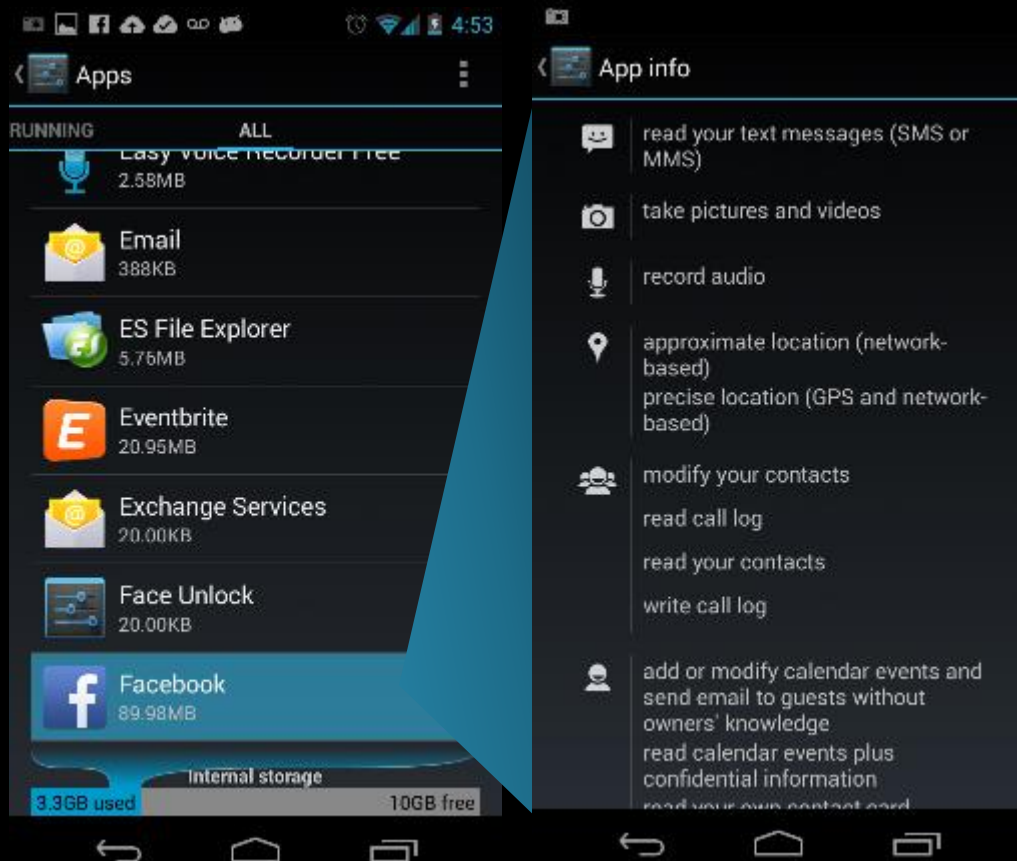






Transparency?

# User Installed Apps vs Ubiquitous IoT



“How do we design interfaces so there’s an intuitive understanding of how public or private a space is?”

Judith Donath  
Harvard Berkman Fellow



Personal data collection should happen  
with knowledge or consent

# Traditional Notice and Choice

Regulators



Normal Users





# Privacy and IoT

## Notice

- Ubiquitous data collection

## Choice

- No interaction models

# Signs Everywhere?

Usability

Does not scale

Limited Information





# IoT Privacy App: Vision

- Gathers IoT privacy preferences
- Proxy for interaction with IoT
  - Nearby devices
  - Cloud

# Scenario: Sensors in a Public Environment





“At a base minimum, people should be able to walk down a public street without fear that companies they’ve never heard of are tracking their every movement – and identifying them by name – using facial recognition technology.”

Statement from Privacy Advocates

June 15, 2015

NTIA process on commercial use of facial recognition technology



“Protecting Photographed Subjects against Invasion of  
Privacy Caused by Unintentional Capture in Camera Images”

[http://www.nii.ac.jp/userimg/press\\_20121212e.pdf](http://www.nii.ac.jp/userimg/press_20121212e.pdf)

# Scenario: Phones/Devices belonging to others



# Scenario: Sensors in the Home/Car



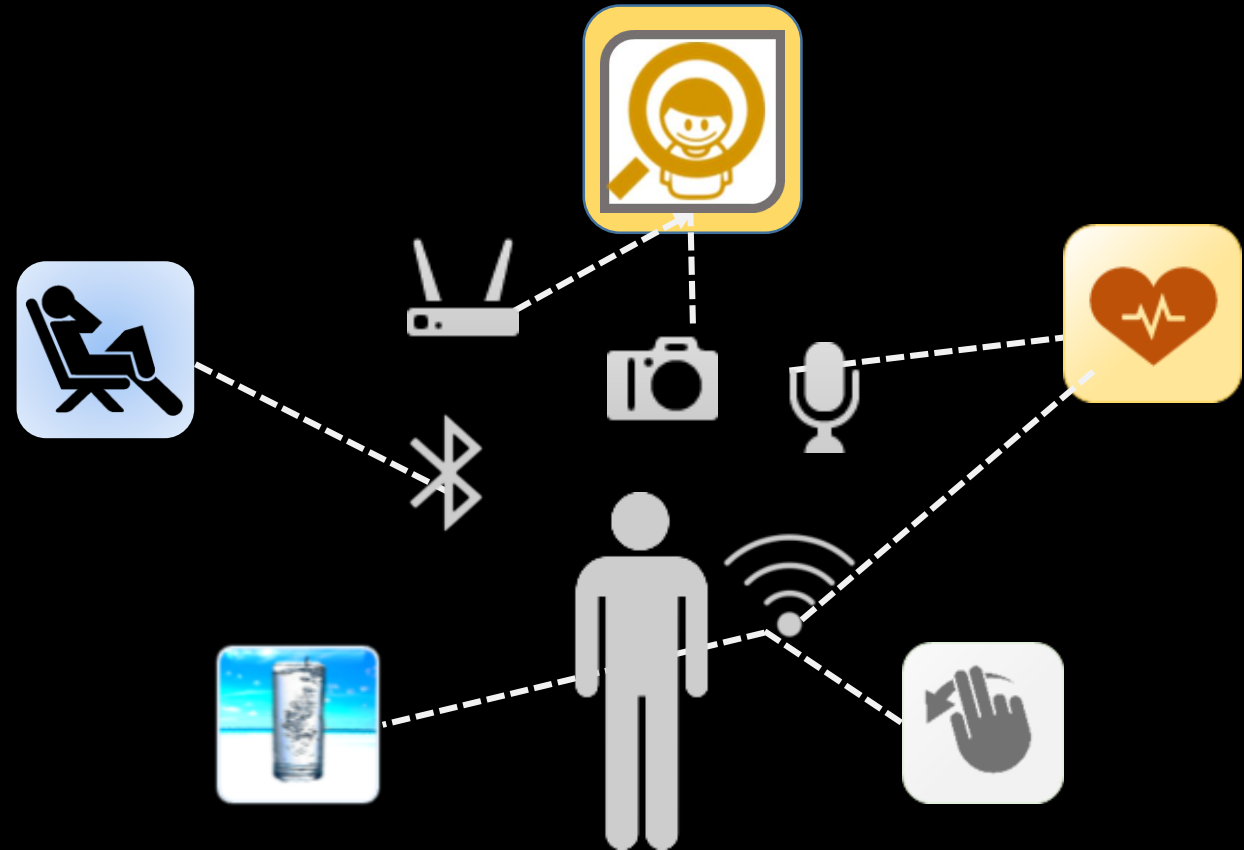


# Scenario: Applications on your phone



# Desired experience

- Discover IoT services
- Filtering for privacy mismatch
- Notify selectively to avoid user conditioning



**Context**



# Absolute Security is Hard

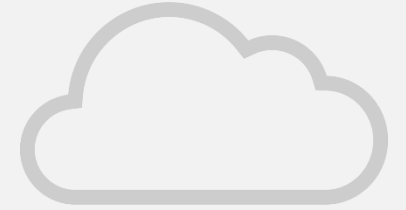
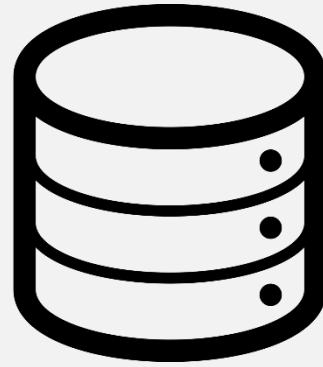
- True adversary can avoid notification
  - Difficult to protect sensors even on your own device
- Relies on:
  - Social norms (devices owned by others)
  - Standards (public sensors)





# System Design

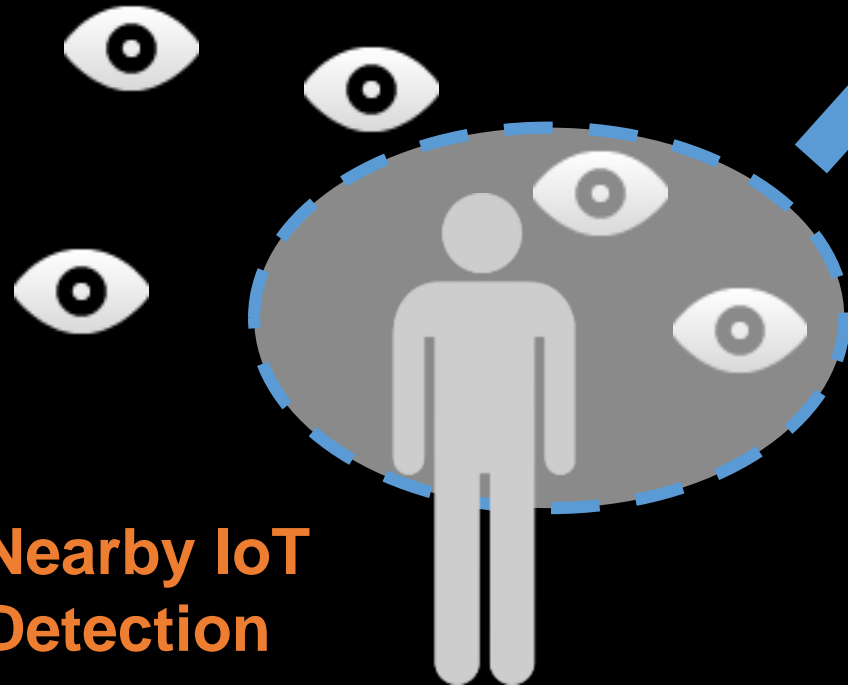
IoT Service Database



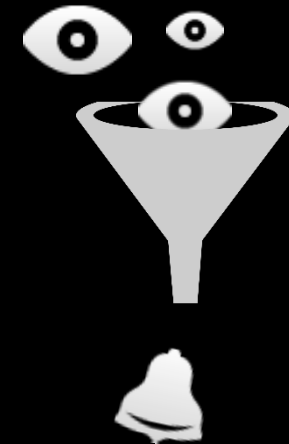
IoT ID

Service Info

Opt in / out



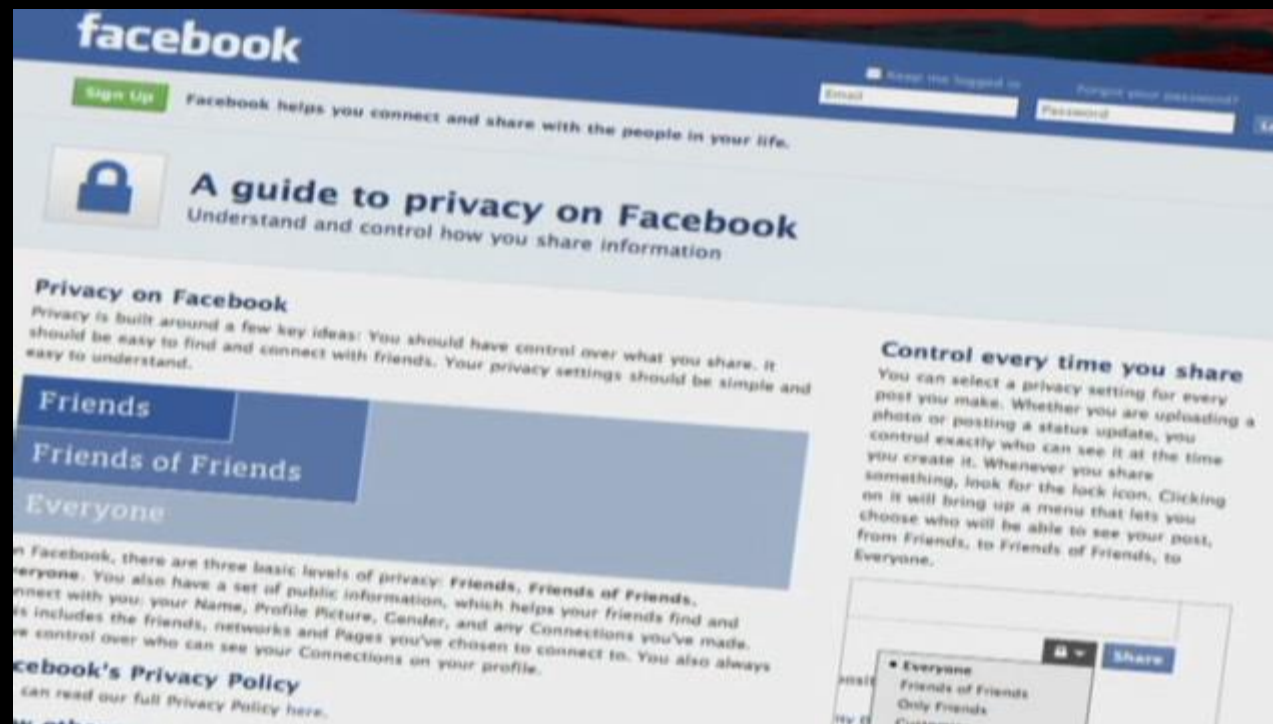
Nearby IoT  
Detection



Privacy Filter  
/ Notification

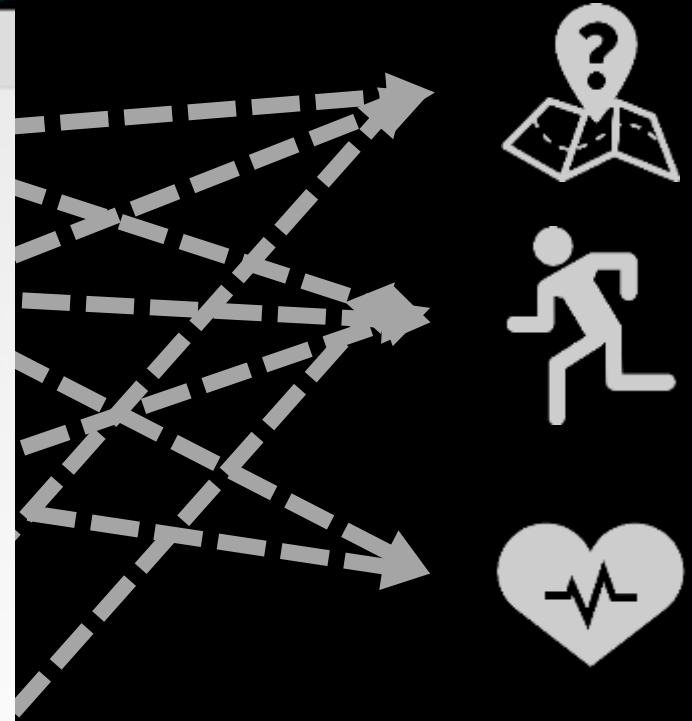
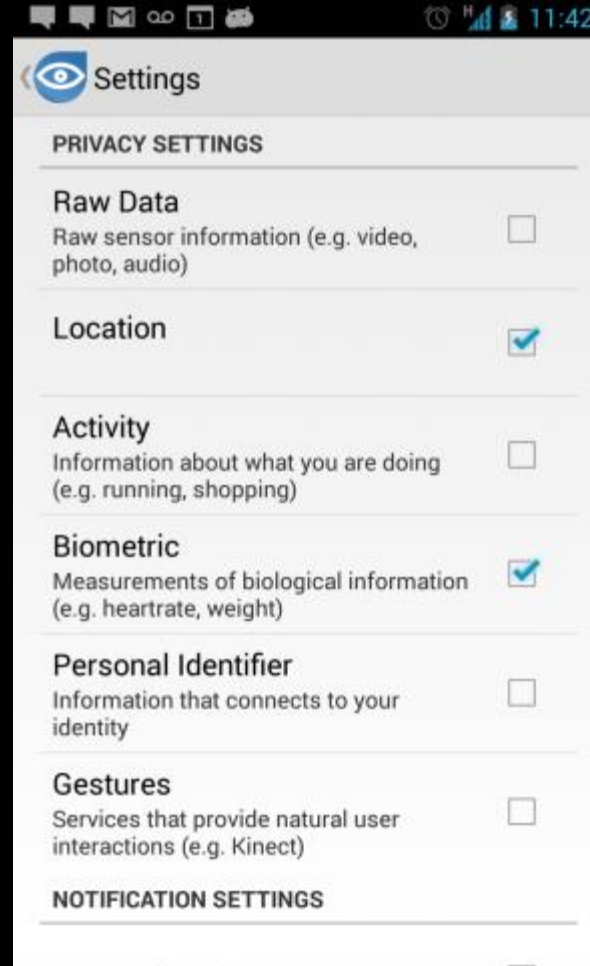
# Challenge: User Interface

Extracting privacy preferences notoriously difficult

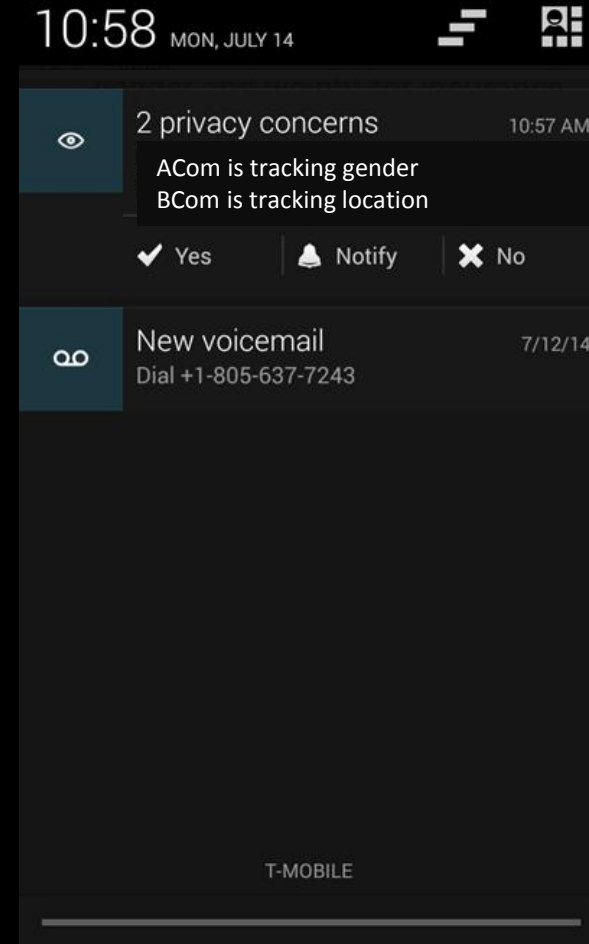
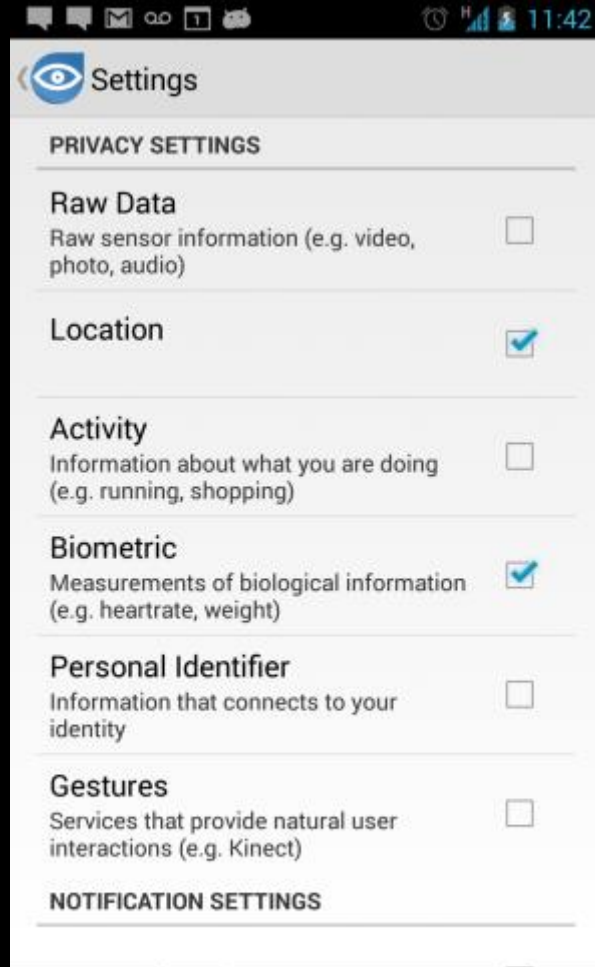




# Filter rules: device data & data inferences



# Privacy filter and notice





# Help from Academia

- Professor Alfred Kobsa
  - “Privacy Decision-Making”
- Intelligent defaults based on machine learning
  - Based on demographics and past behavior
  - Ask what to do for first few cases to gain intelligence



# Challenge: Proximity Detection

- Only nearby devices relevant
- In IoT, how to detect proximate devices?



iBeacon



# Uniformity?



mDNS

# Challenge: Location Privacy



Service queries reveal location

**PROTOTYPE USING AUTO-ID**



# Lookup architecture: Auto-ID

EPC : Electronic Product Code

ONS: Object Name Service

PML: Physical Markup Language



01:00020128:1231293877...

```
<PML>
  <Entity>Starbucks<Entity>
  <Class>
    <Name>mug</Name>
  </Class>
  ...
  ...
  <Part EPC = "01.00011324.1231..." />
  <Measurement EPC = "01.3032.222..." />
</PML>
```

# Add Services to Auto-ID

- Auto-ID: Based on physical objects
- Incorporate
  - Many-to-many mapping
  - Service description and privacy notice
  - Dynamic services

# Service Registration



Developer Account = "012345.678"



Signed  
Package

EPC="01.000501.001..."

SAFE.io



```
<Service EPC="01.000501.001...">  
...  
...  
</Service>
```

# Device Registration



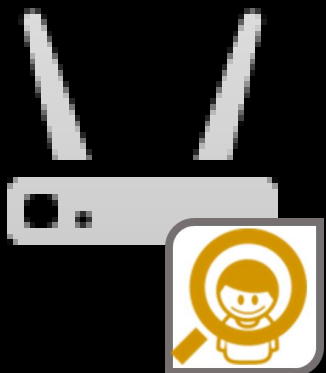
EPC = 00.001405.012{MACADDRESS}

Signed  
Package



```
<PML>
  <Entity><Entity>
    <Device>AccessPoint</Device>
    <Measurements></Measurements>
    ...
  </PML>
```

# Device PML



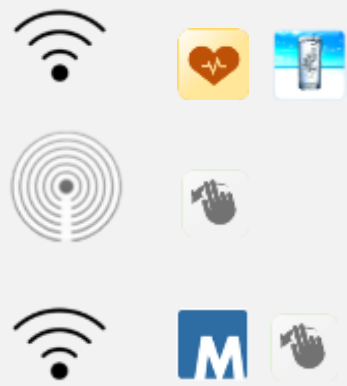
Signed  
Package

```
<PML>  
  <Class>  
    <Name>Access Point</Name>  
  </Class>  
  <Measurements></Measurements>  
  ...  
  <Service EPC =“01.00011324.1231....”/>  
</PML>
```



```
<Service EPC =“01.00011324.1231....”>  
  <Name> KinderFind </Name>  
  <Developer> Safe.io </Developer>  
  <Description>.....</Description>  
  ...  
</Service>
```





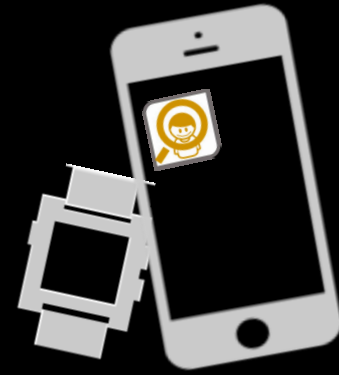
Device  
EPC

PML



```
<PML>  
<Entity>IT Department<Entity>  
<Class>  
<Name>Access Point</Name>  
</Class>  
<Service EPC = "01.00011324.1231..." />  
</PML>
```


MACADDRESS  
EPC = 00.001405.012{MACADDRESS}

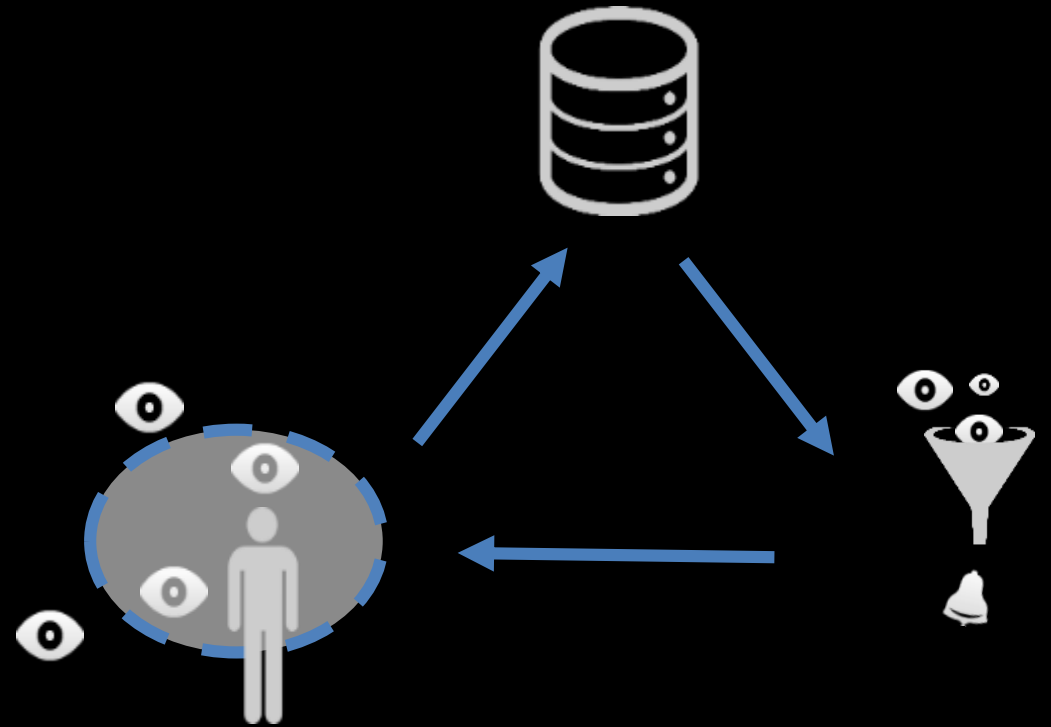


Nearby IoT Detection

IoT Service Listing

# Recap

- IoT  Big Data
- Need unified frameworks and interfaces
- Issue: User control and transparency



# **UC IRVINE: USER ATTITUDES**

# User Privacy Attitudes towards IoT

- Which parameters are important?
  - [who]
  - [what]
  - [reason]
  - [where]
  - [persistence]
- Randomly generated IoT scenarios varying these parameters
  - (Qualitative) Interview study w/ 10 participants
  - (Quantitative) Amazon MTurk survey study w/ 200 participants

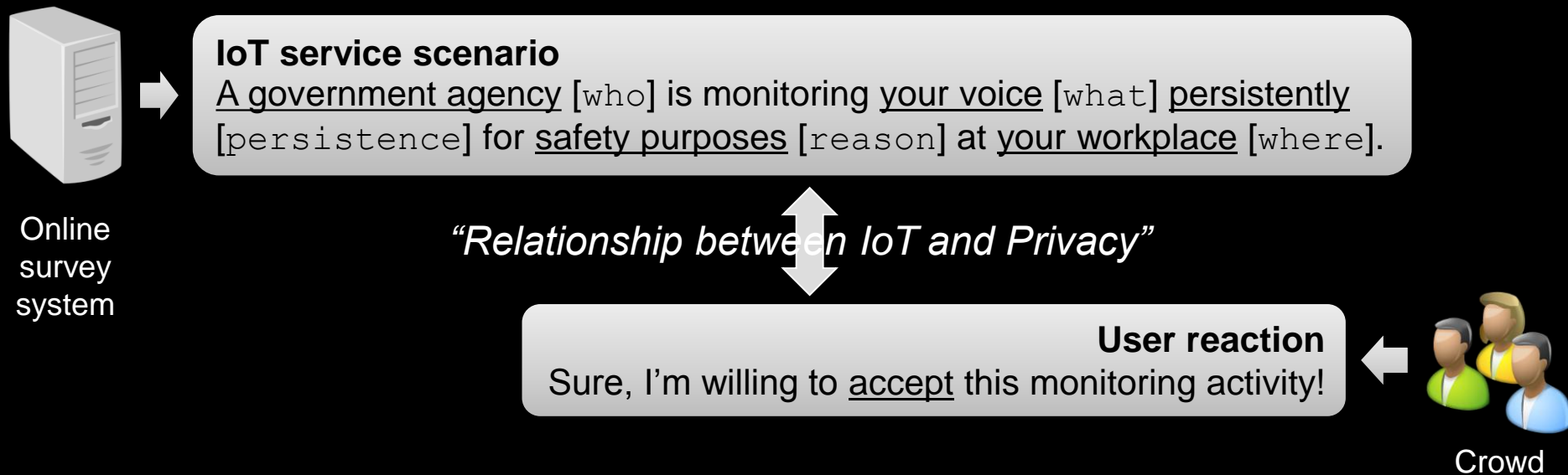
# Interview Study

- For various scenarios, participants were asked whether they
  - Felt comfortable
  - Wanted to be informed
- Responses
  - Main reasons to feel uncomfortable
    - Unreasonable/suspicious purpose of data collection [reason]
  - Main reasons to feel comfortable
    - Trustable entity who collects data [who]
    - Purpose justifying data collection [reason]



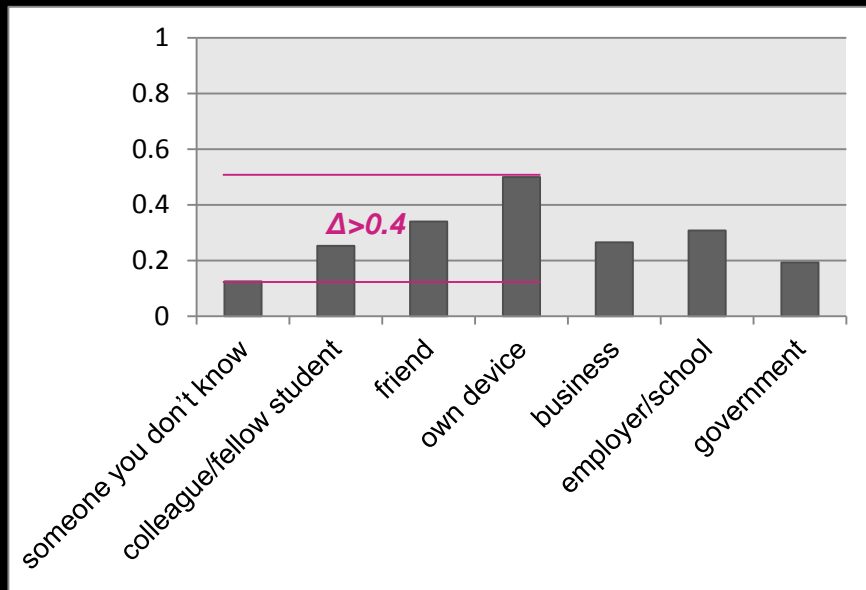
# Online Survey Study

- Overview
  - How user attitudes differ based on parameters?

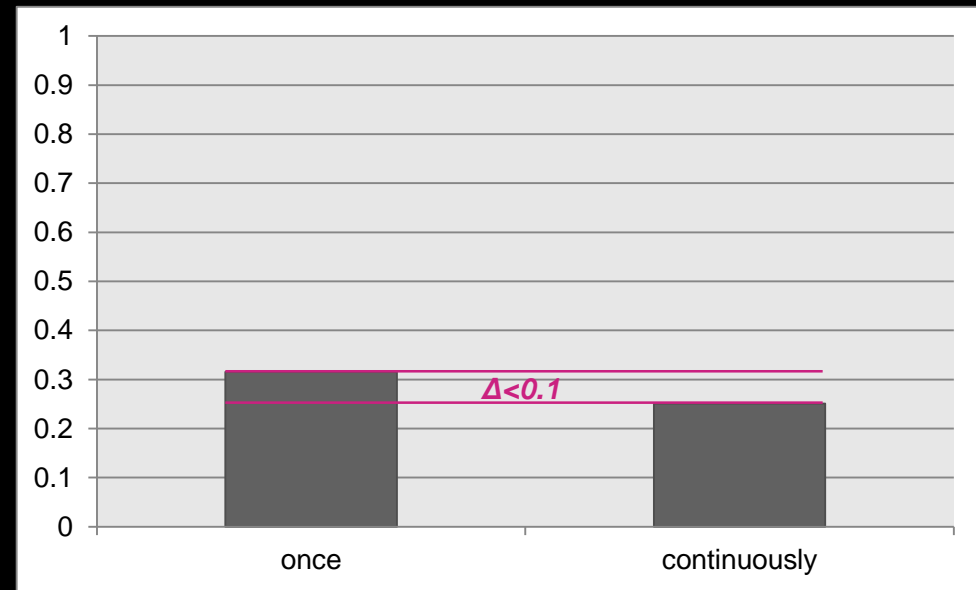


# Online Survey Study

- Result #1
  - Most significant factors influencing user reactions are [who] and [what]
  - Relatively, [reason], [where] and [persistence] have less impact



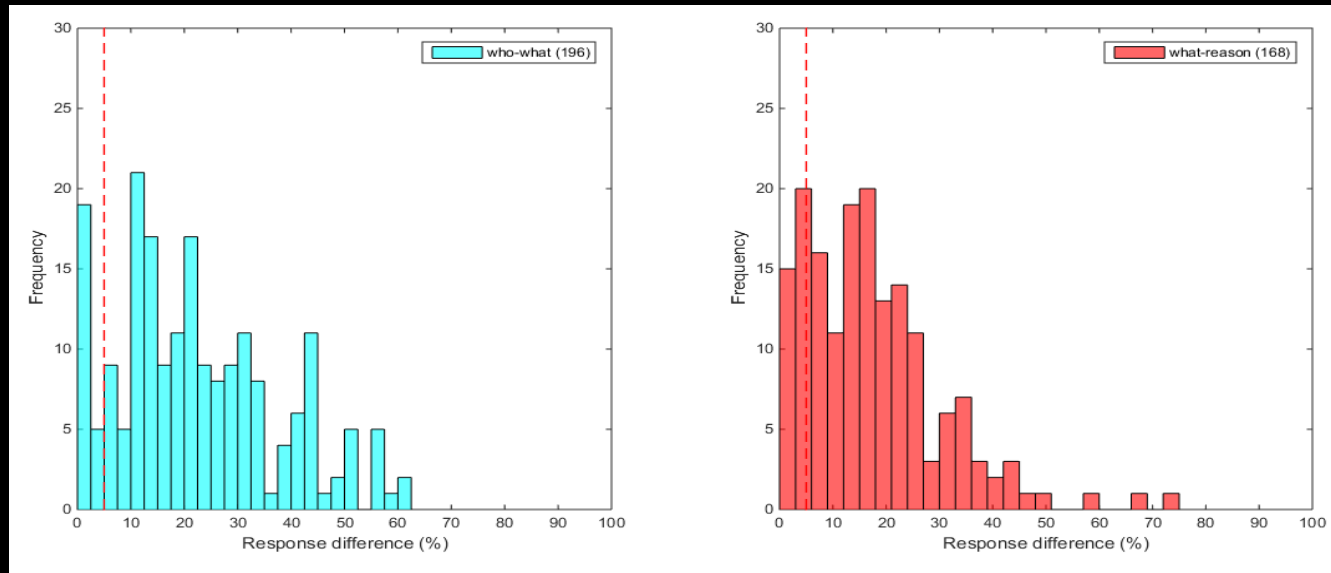
Agreement to being monitored (1: allow, 0: not allow),  
broken down by [who]



Agreement to being monitored (1: allow, 0: not allow),  
broken down by [persistence]

# Online Survey Study

- Result #2
  - [persistence] has a noticeable impact in subspaces of the scenarios



*Difference in agreement to monitoring,  
broken down by [persistence]*

- Implications
  - [who] and [what] are affecting people's privacy decisions globally
  - [persistence] interacts with [who]-[what] and with [what]-[reason]

**UC BERKELEY: HOW TO NOTIFY?**



REALSENSE™  
TECHNOLOGY

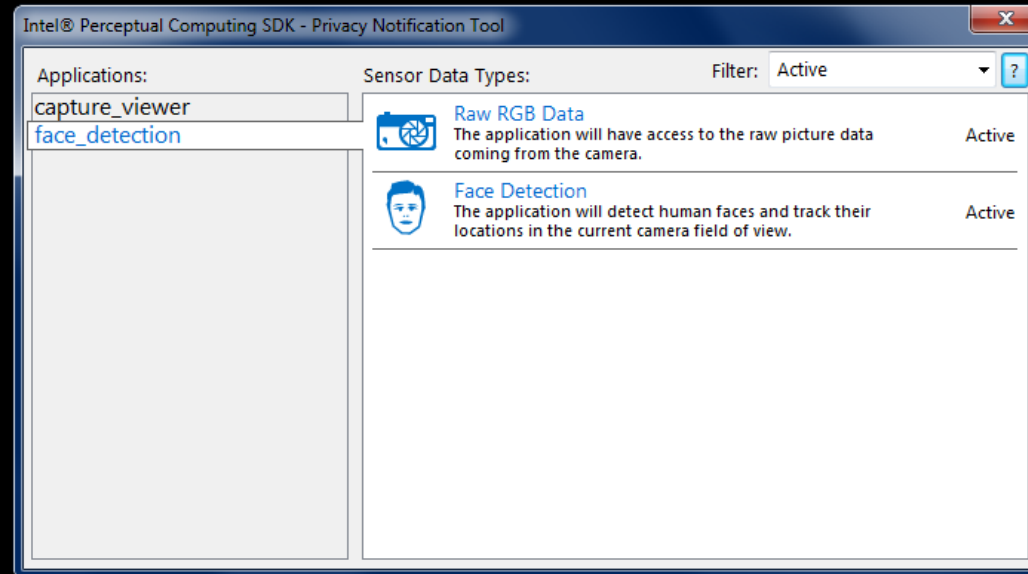
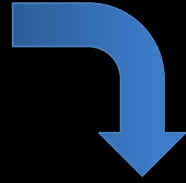
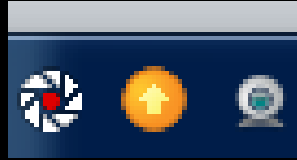


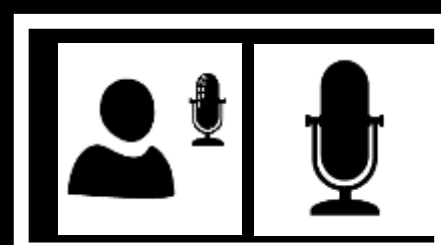
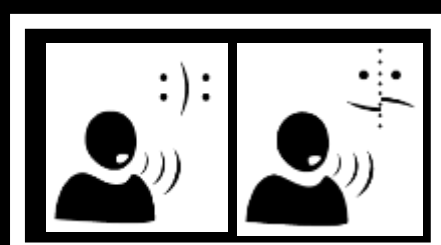
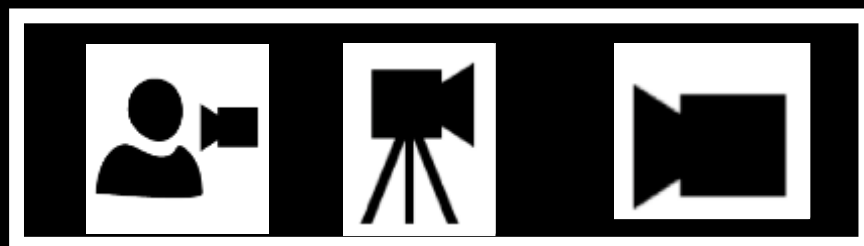
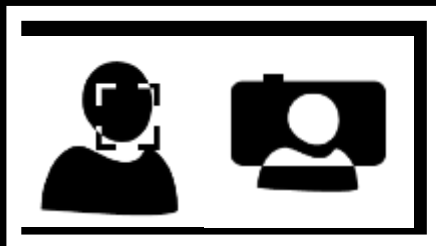
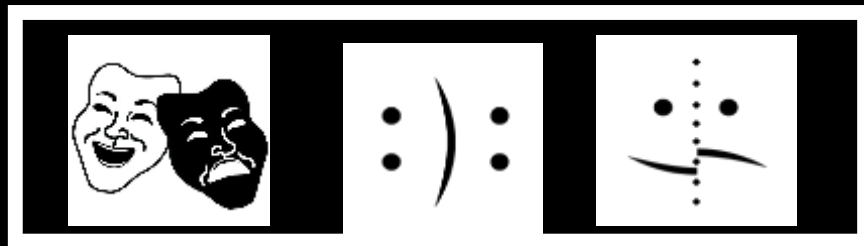
# RealSense / Perceptual Computing

apps can use camera/mic for audio/video

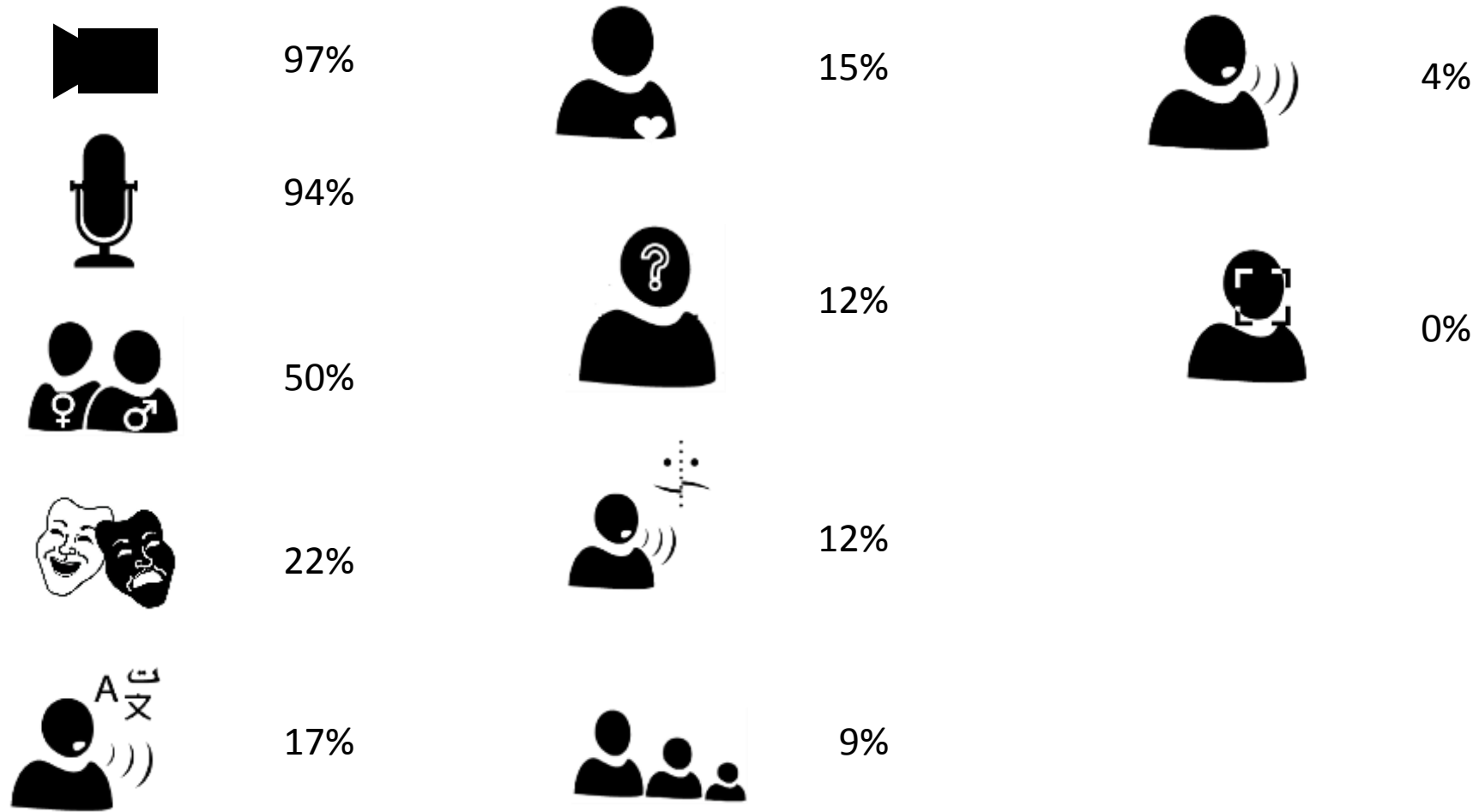
or...

- face-based age detection
- face-based emotion detection
- face-based gender detection
- face detection
- face recognition
- voice command & control
- speech to text
- language detection
- gesture recognition
- voice-based emotion detection
- eye tracking
- heart rate monitor





# comprehension varied...



crowdsourcing icons

## Instructions



Using the drawing widget on the right, please draw an icon to depict the following concept:

### ***Speech to Text***

The microphone will capture audio and convert it to text, and then allow various applications to access this text. However, no applications will have access to raw microphone data (i.e., audio from the user).

#### *Example:*

A smartphone application allows the user to dictate text or email messages, so that they do not need to touch the device while driving.

## 1. Drawing Widget



Erase Everything

## 2. Please describe your drawing:

Submit HIT



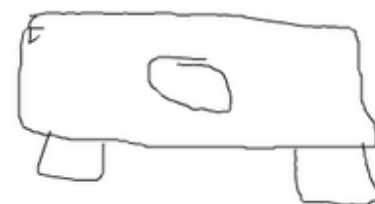
**1: Video Recording (A177EXELDLWTWV)**

A different colored recording icon



**2: Video Recording (A177KOH91KZYU)**

like the one in the movie odyssee of space, that was clearly looking at you



**3: Video Recording (A19RQWEFUEB1QU!U)**

video camera



**4: Video Recording (A1C19XPG91AIXX)**

The red circle is what I think of when I think of the word "recording"



**1: Audio Recording (A11PYN5E5MEMV7)**

The picture is a microphone, with sound waves entering the front of it. The color is red, because it's a very noticeable color and anybody could see it easily



**2: Audio Recording (A1A8LG09ZLYLKX)X)**

Talking mouth in a bubble



# example themes

- **age detection** (16)
  - child and/or adult (10)
  - heart (14)
  - EKG (11)
- **emotion detection** (13)
  - smiley face (9)
- **gesture recognition** (11)
  - hand (10)
  - waving motion (6)
- **gender detection** (14)
  - male/female symbols (7)
- **speech to text** (15)
  - letter (11)
  - sound wave (7)
- **face recognition** (16)
  - face (14)
  - crosshairs/frame (10)
- **heart rate** (20)

# final icons (n=300)



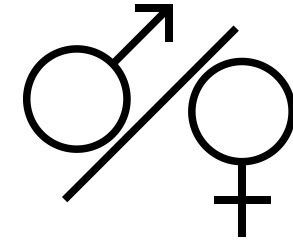
99%



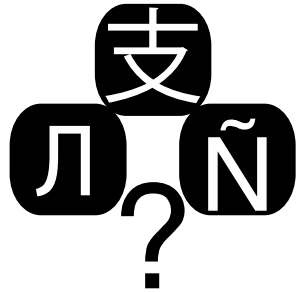
99%



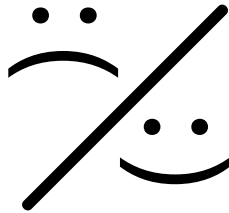
99%



96%



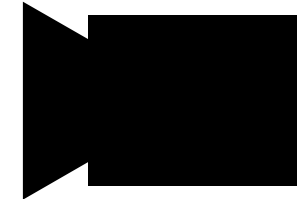
91%



91%



86%



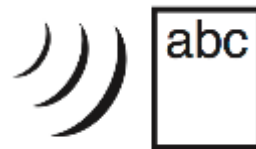
86%



85%



79%



73%



44%

Questions/Comments?

[richard.chow@intel.com](mailto:richard.chow@intel.com)