Usable Privacy Policy and Personalized Privacy Assistant Projects

Session III: Personalized Privacy Assistants for Mobile and IoT

Instructors:
Anupam Das, Martin Degeling and Norman Sadeh
Carnegie Mellon University

usableprivacy.org privacyassistant.org
explore.usableprivacy.org

What If….

- **Computers understood privacy policies?**
- **Computers understood** what we **care about** and what we **already know/expect**

Session III Outline

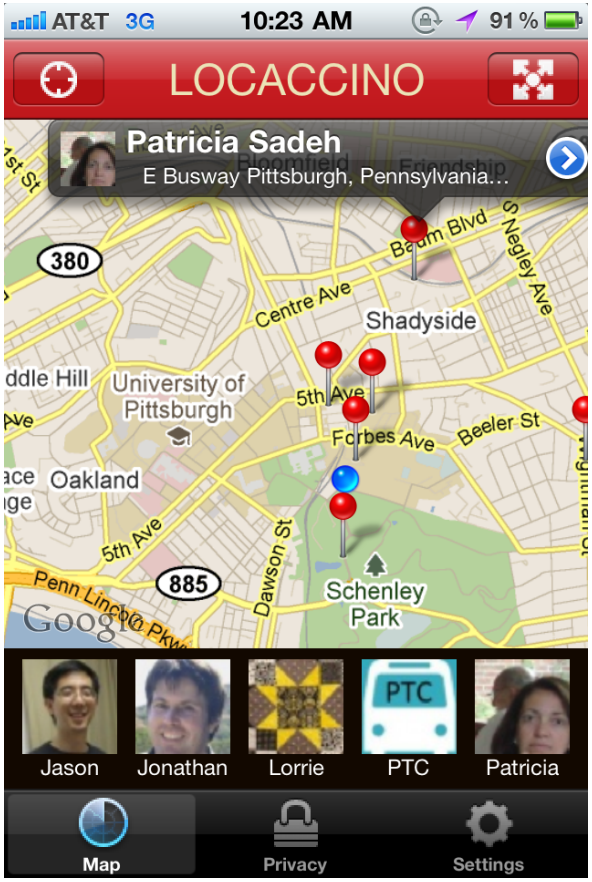
- Understanding Mobile App Privacy Preferences
- Learning People's Mobile App Privacy Preferences
- Mobile App Privacy Assistants
- IoT Privacy Preferences
- IoT Privacy Assistants & Infrastructure

Questions/Challenges

- What types of privacy preferences should we try to learn?
- Do people know their privacy preferences? Can we just ask them?
- Can we learn people's privacy preferences by observing them?
- How similar/diverse are people's privacy preferences?
- How stable are people's privacy preferences?

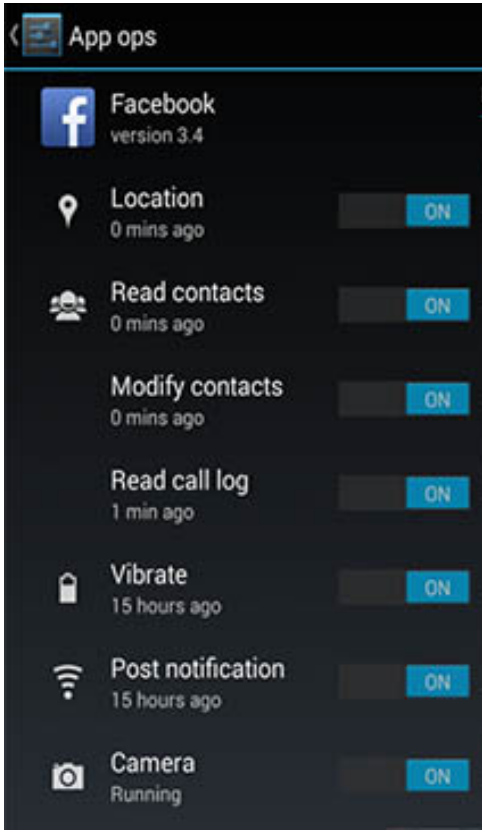
Historical Perspective - I

- Early work in MyCampus (2001-2006)
- Work on **location sharing** privacy preferences (2006-2012)
  - Comfort sharing one's location with others, under what conditions, at what level of granularity, etc
  - Exploring expressiveness and user burden tradeoffs
  - Learning people's privacy preferences (e.g. privacy profiles)



Historical Perspective - II

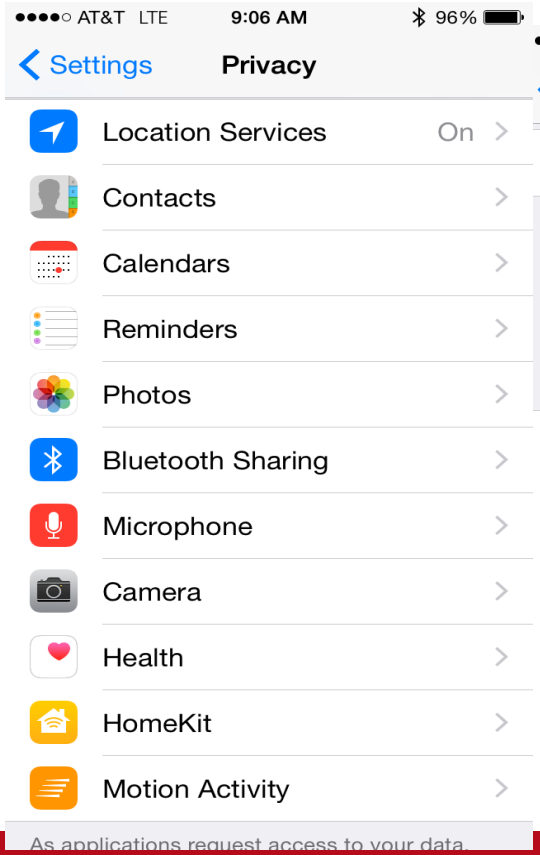
- Later moved to mobile app permissions (2011-present)
- …and most recently richer IoT privacy preferences (2014-present)
  - no longer just disclose vs. do not disclose
  - But also
    - retention, purpose, sharing, aggregation, etc
    - Notification preferences and expectations

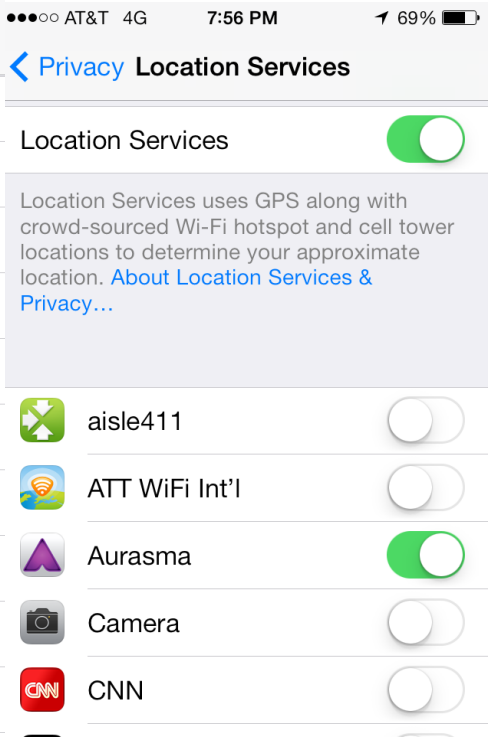


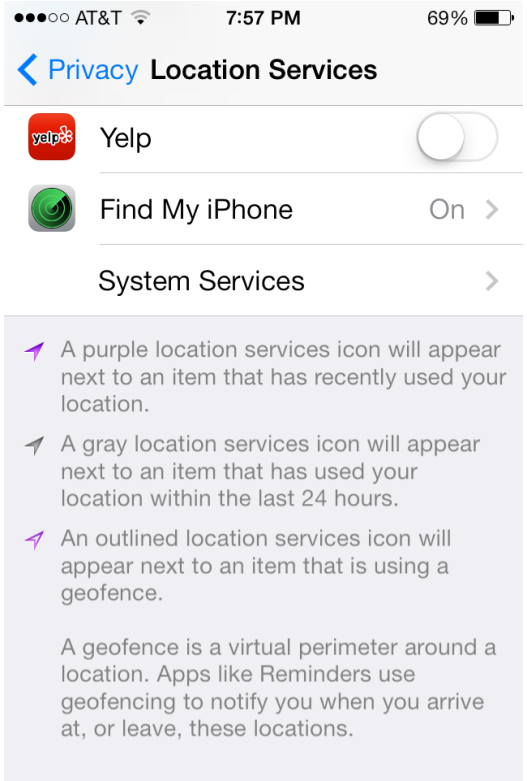
Understanding People's Mobile App Privacy Preferences

Explosion in Number of Privacy Settings (iOS)

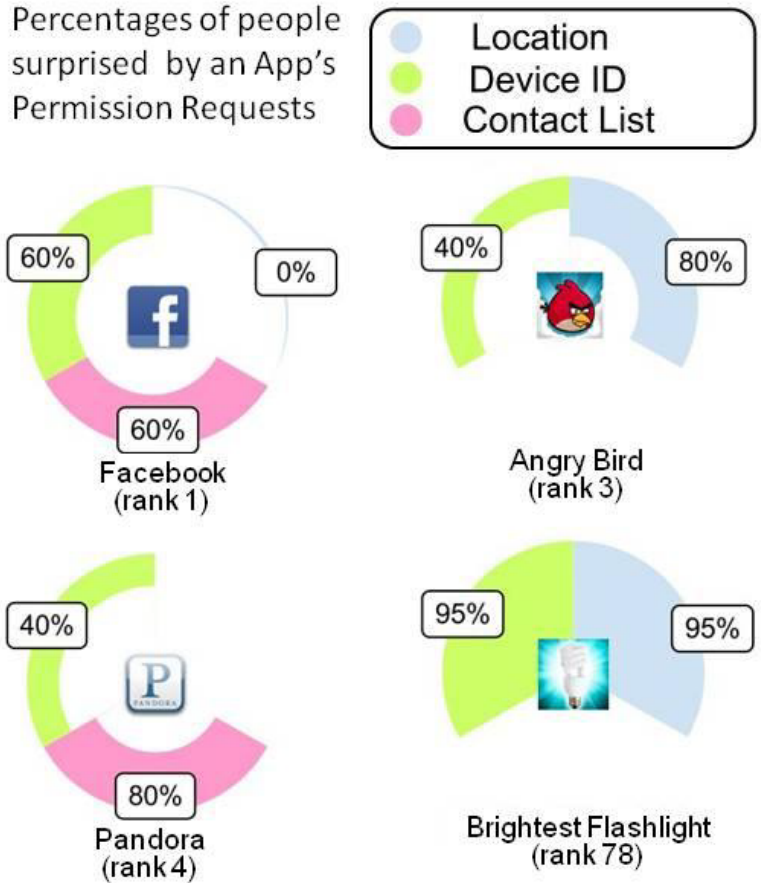
A few iOS8 privacy screens – not even all location permission screens!







People Are Often Unaware of their Permission Settings

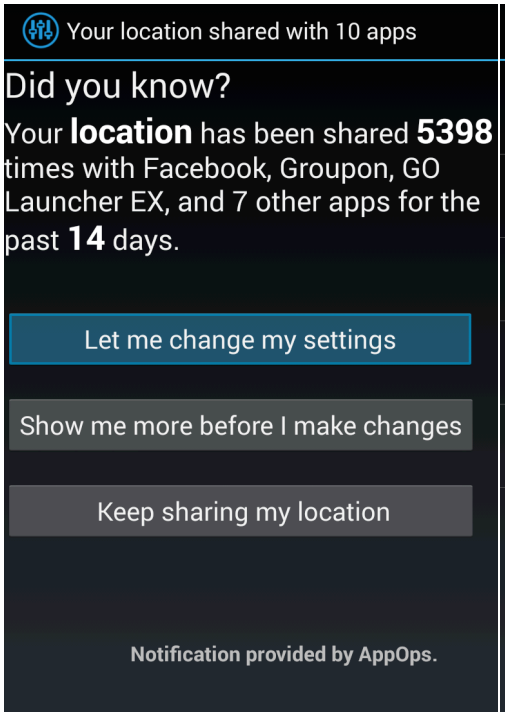


- **Privacy as a secondary task**
- Lack of mechanisms to engage people and motivate them to look at settings
- Unexpected collection & sharing are widespread

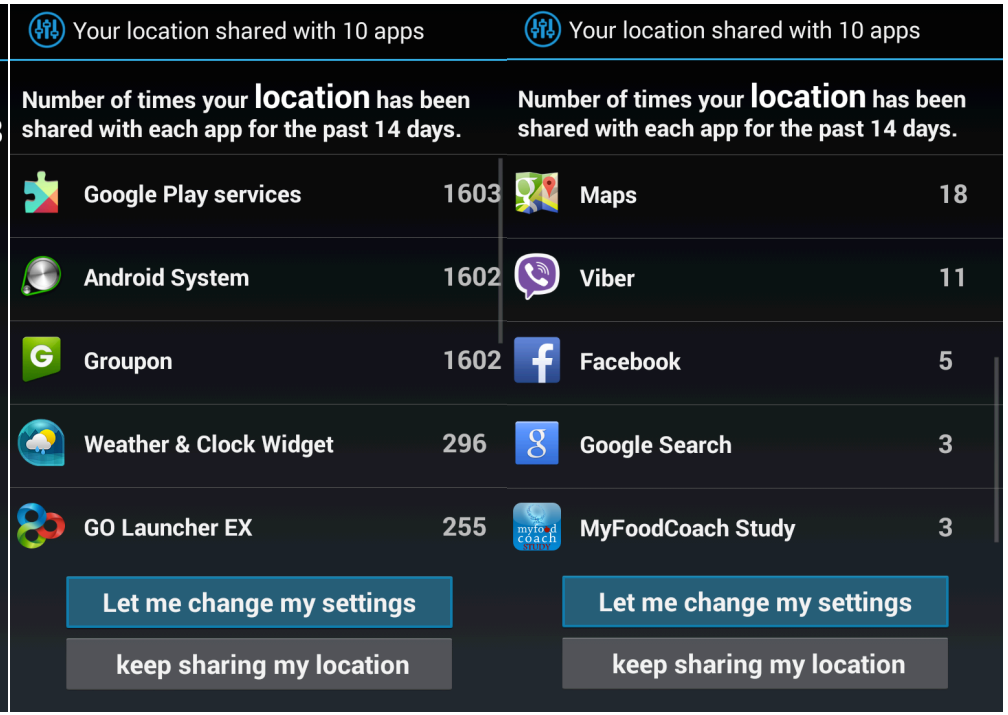
J. Lin, S. Amini, J. Hong, N. Sadeh, J. Lindqvist, J. Zhang, "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing", Proc. of the 14th ACM International Conference on Ubiquitous Computing, Pittsburgh, USA, Sept. 2012

Nudging Users to Engage with Settings

Privacy Nudge



Detailed Report



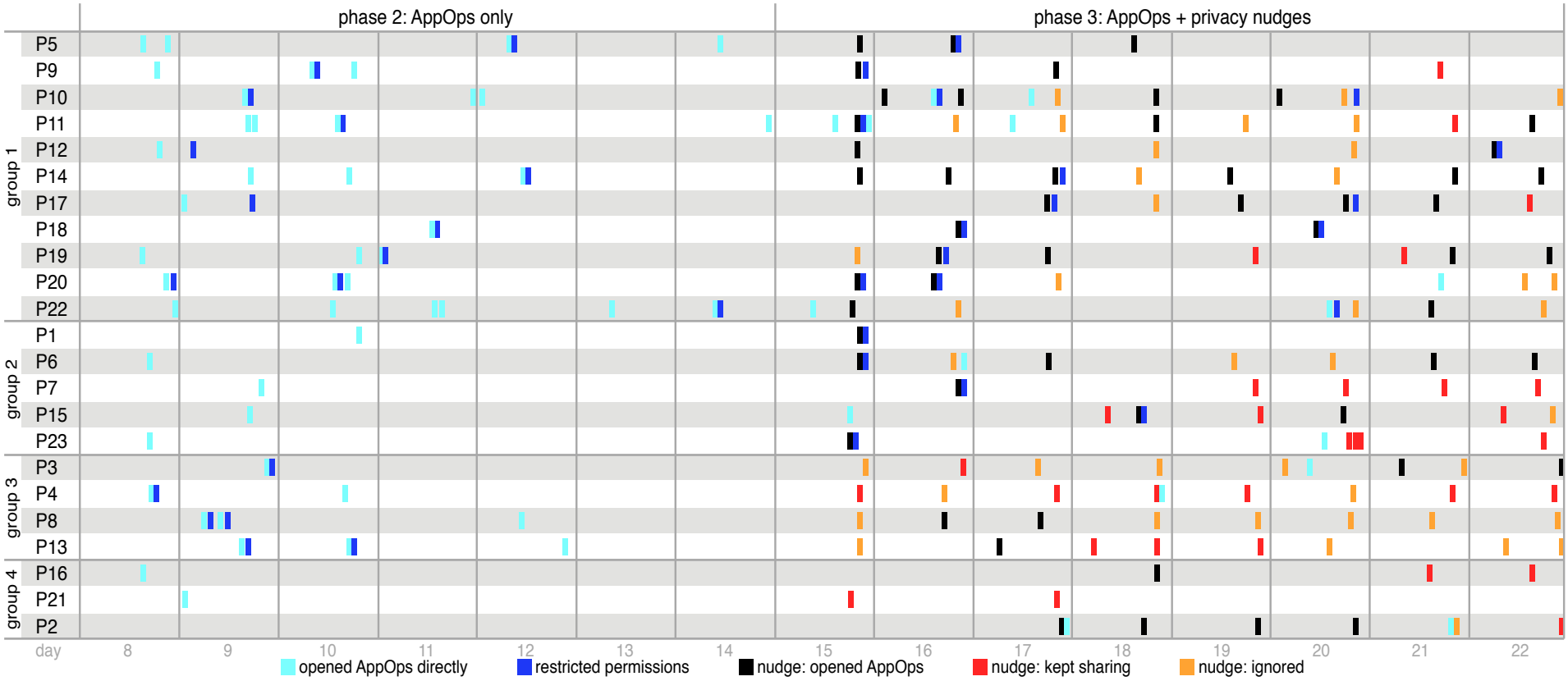
Field Study

- 22-day study with 23 participants using their regular Android phone
- **Week 1:** baseline – no access to App Ops
- **Week 2:** App Ops (email & SMS)
- **Final 8 days:** App Ops + one daily nudge focused on one permission
- Collected detailed logs of all permission changes + pre- and post-surveys

Demographics

- **23 participants** (65% female; ages 18–34, median=23)
  - 21 owned Samsung devices and 2 owned an HTC One.
- On average, 89 apps installed (SD=22), including services and pre-installed apps.
- **21 (91%) reported never using AppOps before**
  - 1 had used AppOps, and 1 was unsure.
  - Phase 1 showed that participants could not access AppOps until phase 2 (e.g. no other launcher app for AppOps installed).

Overview of participants' interactions with AppOps and the privacy nudges



App Permission Manager w/o Privacy Nudges (Phase 2)

- **22 (out of 23) participants (95.6%) reviewed** their app permissions at least once
- 15 (**65%**) participants restricted **272 app-permission pairs from 76 distinct apps**, including both participant-installed and pre-installed apps.
- Only one interaction where a user opened access to one permission.
- **Conclusion: Permission Managers Help**

Adding Privacy Nudges – Final 8 days (Phase 3)

Do nudges further change user behavior and how do users feel about them?

Effectiveness of Privacy Nudges – Final 8 days

- In phase 3, participants reviewed their app permissions **69 times**, restricted **47 distinct** apps from accessing **122 app-permission pairs**, and permitted six apps access to six permissions.

- ….**this is after a week with access to App Ops.**

Reviewing App Permissions

- Participants could review their app permission either by
  1. **opening AppOps directly** (same as in phase 2)
  2. **opening AppOps in response to a nudge**

Reviewing App Permissions

- 22 participants (95.6%) reviewed their app permissions at least once in phase 3.
  - **21 participants reviewed their apps' permisions in**

The privacy nudges were the primary trigger for participants to review their app permissions.

  - **1 participant** reviewed her apps' permissions only once and **only by directly opening AppOps**

Observations

- **Privacy Nudges** can help increase user awareness and **motivate users** to review their privacy settings
- Using settings from users who have received privacy nudges is **more likely to reflect their "true" preferences**
  - *Less likely to result in regret*
- But the **number of mobile app permissions remains overwhelming**

Mobile App Privacy Assistant*

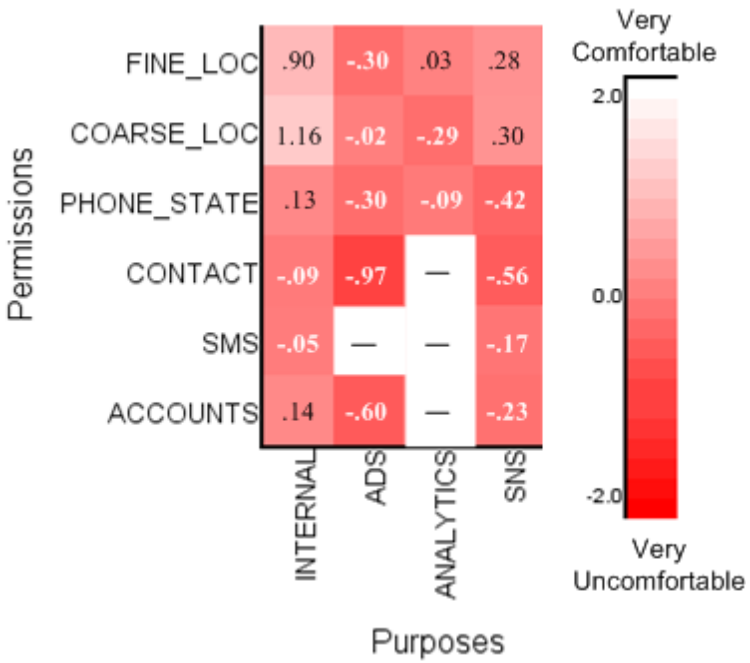
- Could we learn people's privacy preferences?
- Different possible models:
  - Learn privacy profiles from a collection of people, and assign users to **profiles** to generate recommendations
  - Learn **from a user's existing settings** (e.g. as user download more apps, start making some recommendations)
  - **Combine both models**
  - Another dimension: **recommend vs. configure**
  - Not just configuration of settings but **also notification**
    - **Including frequency, manner, etc.**

* Patent pending

Configuring Privacy Settings

- Learn People's Mobile App Privacy Preferences
  - Including **analysis of permission purpose**, using code analysis
- Build **Privacy Profiles** (clusters of users)
- Ask **each user a few questions to identify a profile that best matches their preferences**
- Based on their profiles and the apps on their smartphones, **recommend settings**

Android Permissions: **Purpose Matters!**

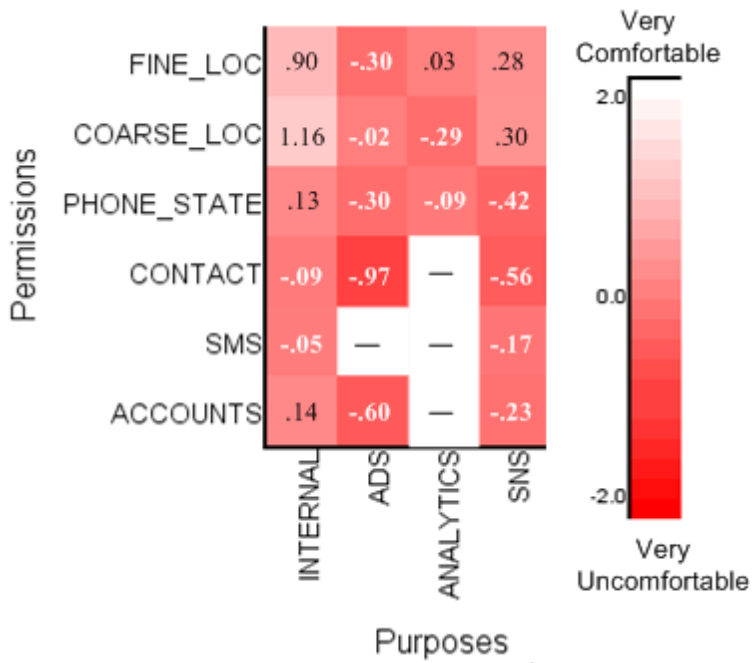


Users' Average Preferences

White → comfortable
Red → uncomfortable

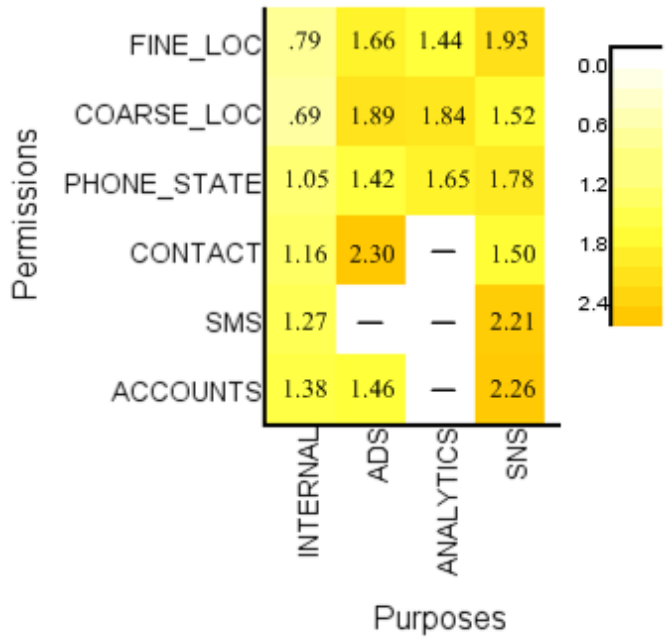
J. Lin, B. Liu, JN. Sadeh, and J.I. Hong, "Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings", 2014 ACM Symposium on Usable Security and Privacy (SOUPS 2014), July 2014.

One Size-Fits-All Defaults Don't Work



Users' Average Preferences

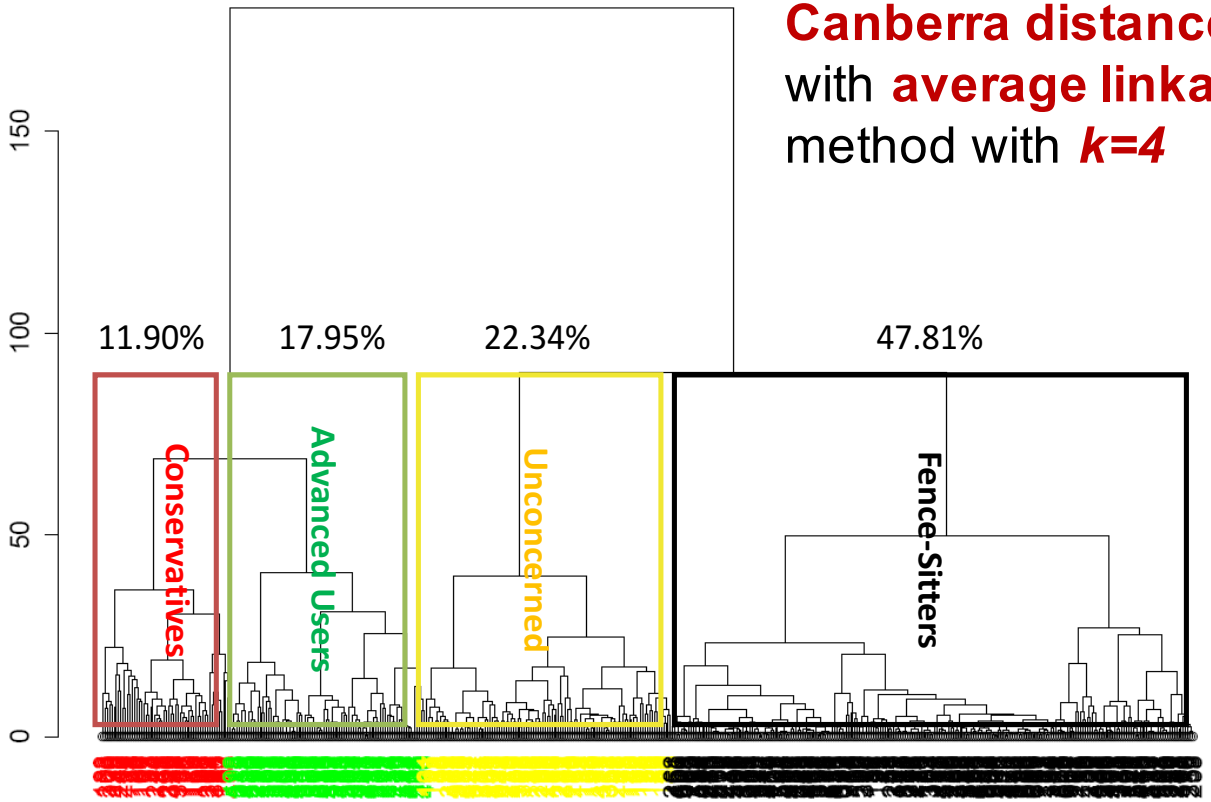
White → comfortable
Red → uncomfortable



Variance among Users

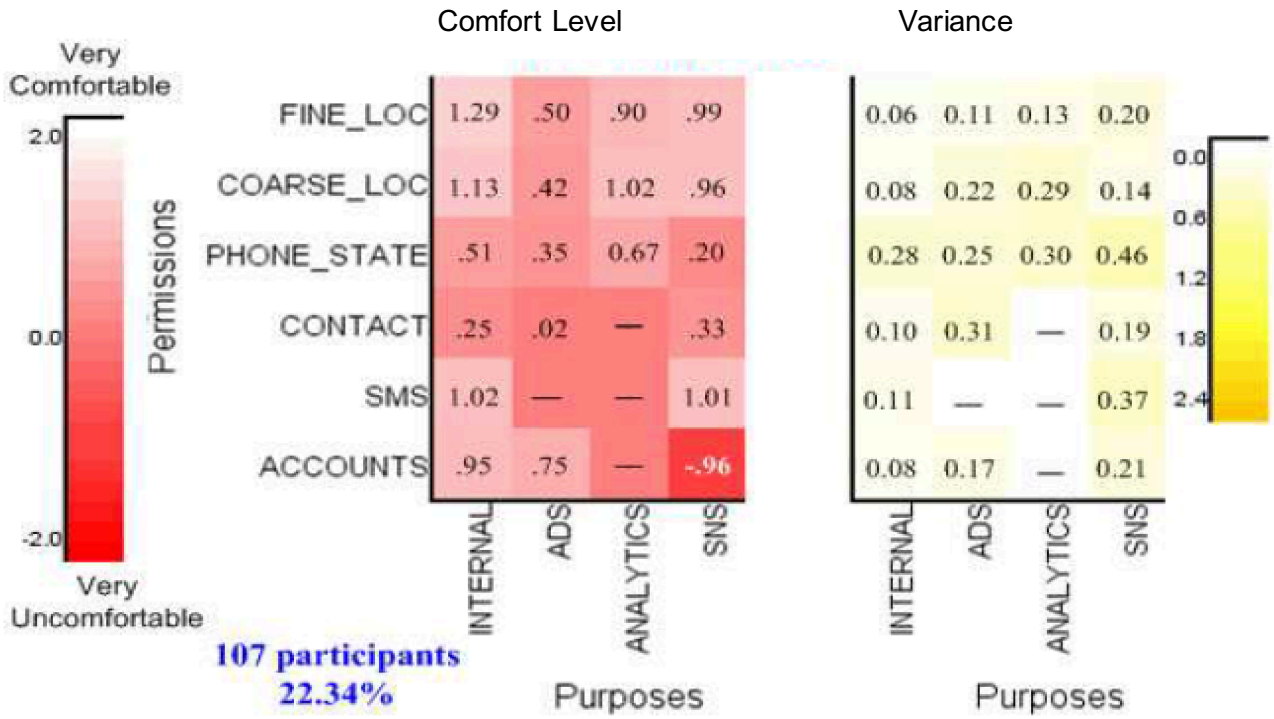
Darker yellow → larger variance

Hierarchical Clustering



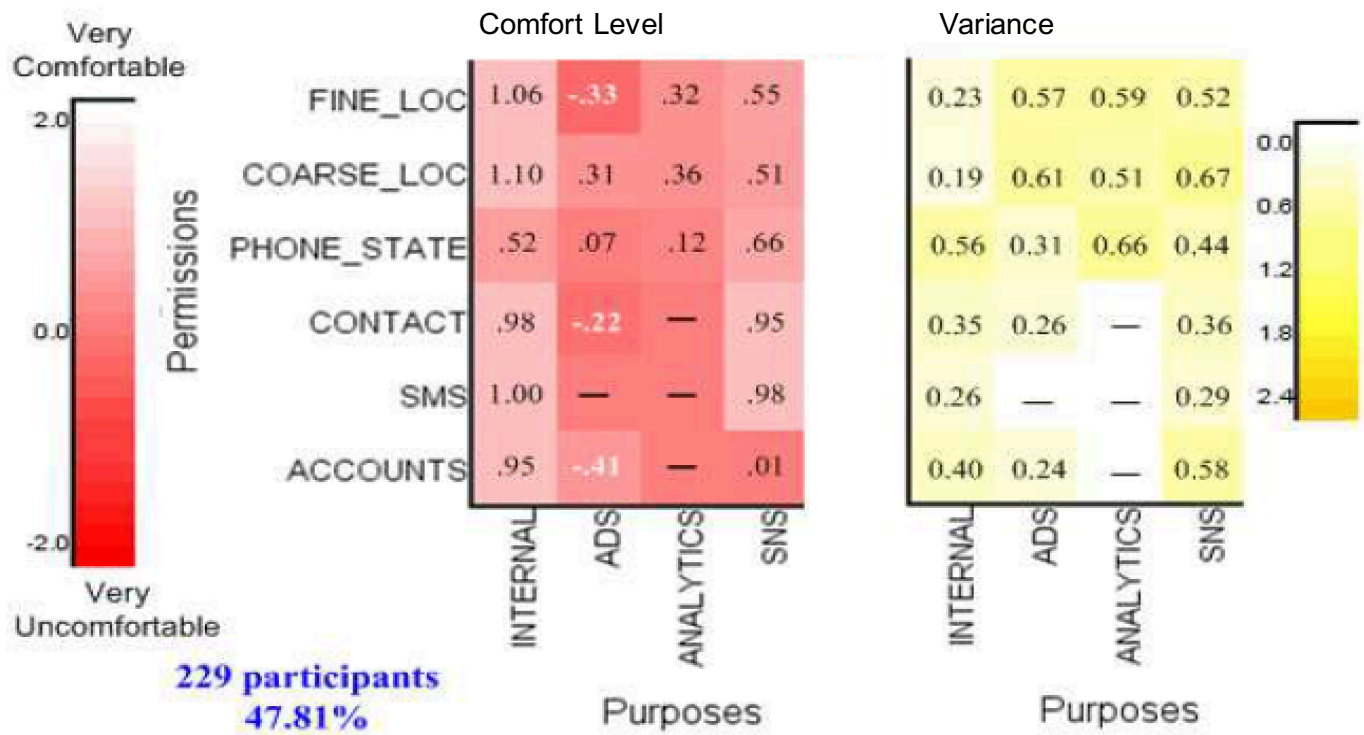
Canberra distance with **average linkage** method with ***k=4***

Unconcerned Cluster



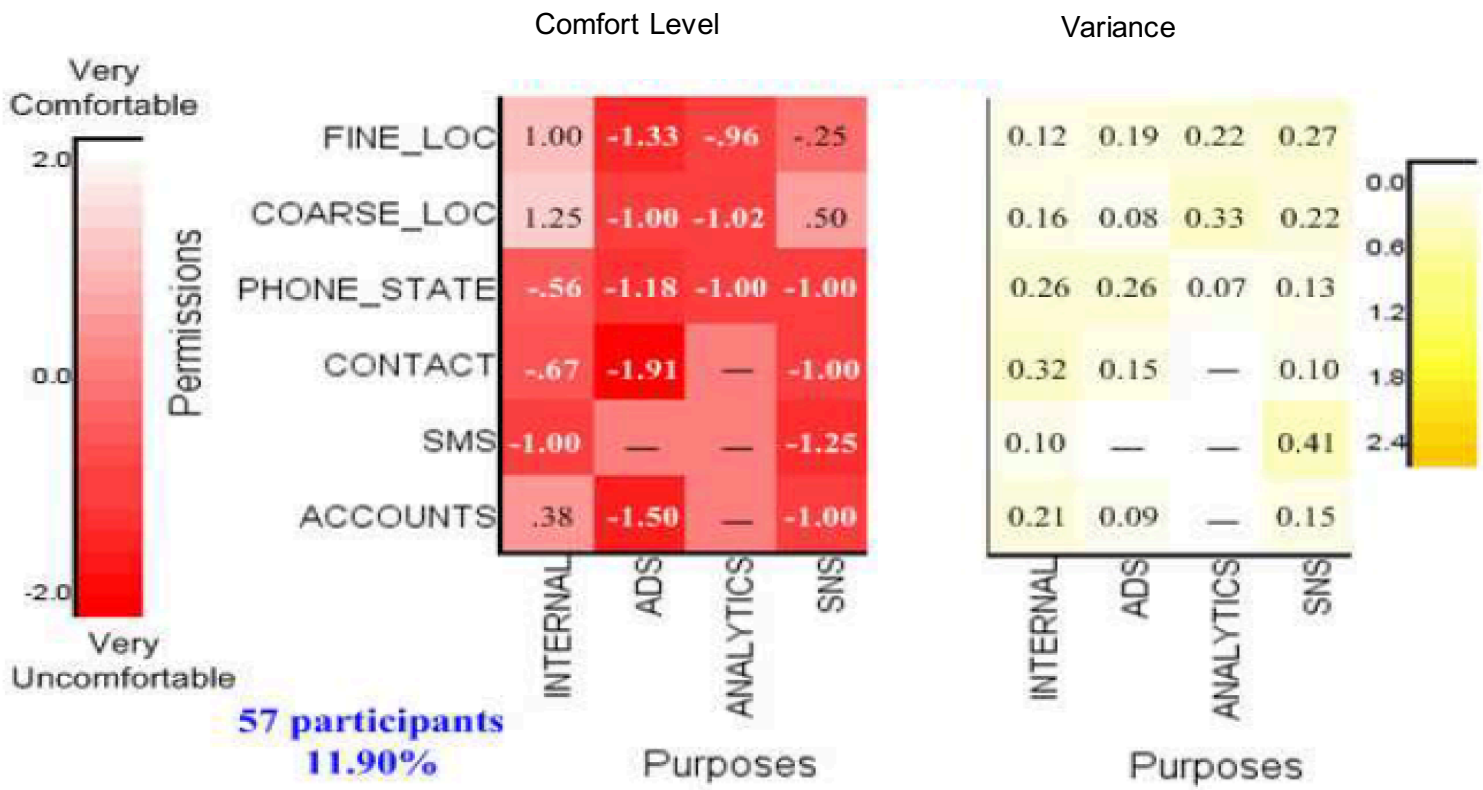
- Generally open to all types of disclosures
- Red in SNS/Accounts is probably a fluke – insufficient data

Fence-Sitters



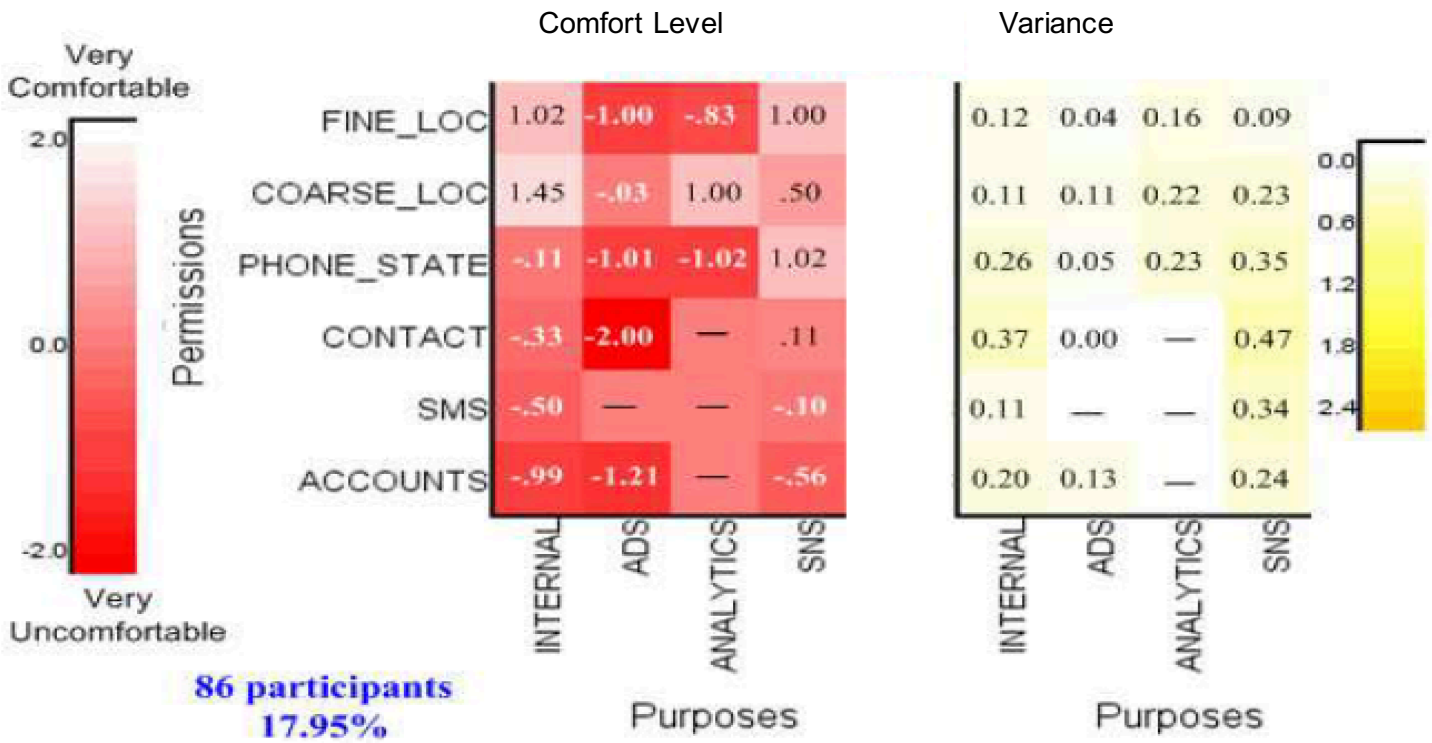
- Largest group of users (47.81%)
- Seem to have relatively neutral attitudes – could be habituation

Conservatives



- Uncomfortable letting external libraries access their information in general
- Even for internal purposes in the case of contact list, SMS and phone state

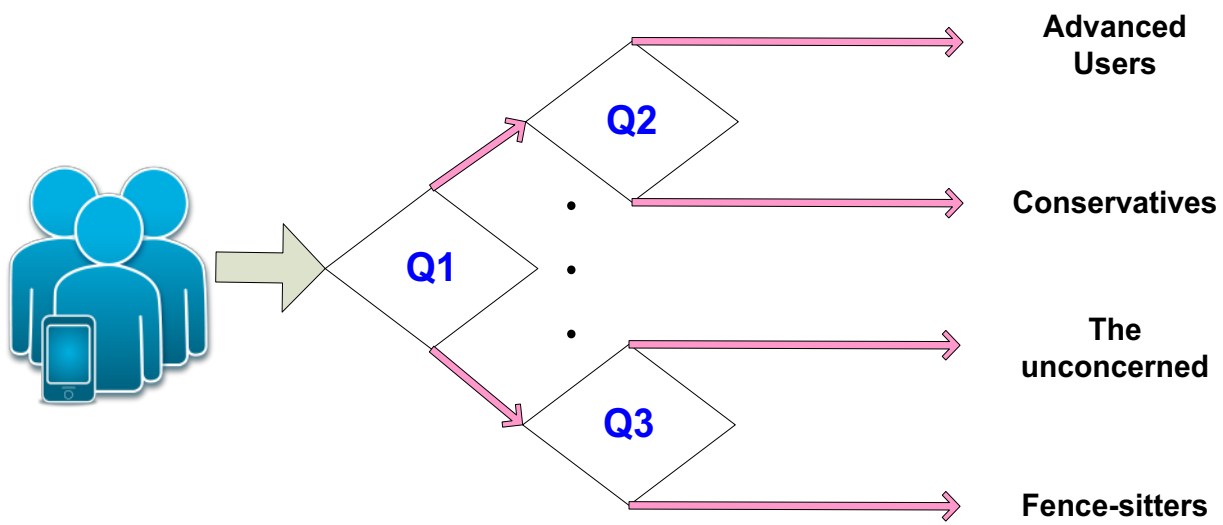
Advanced Users



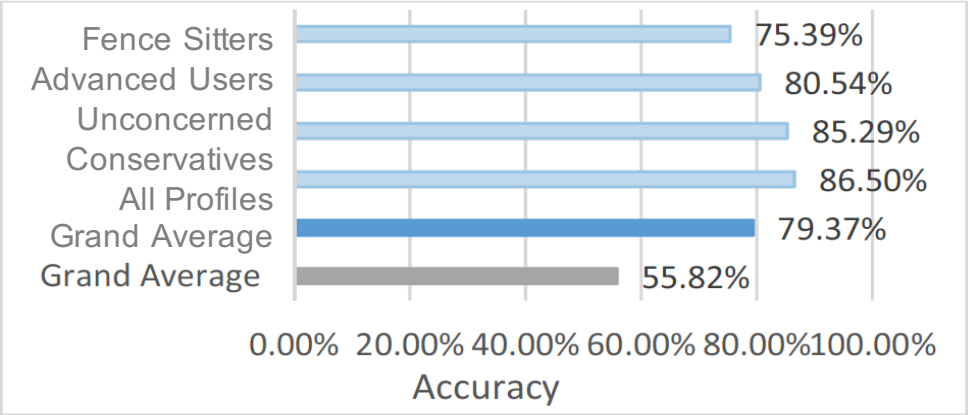
- Don't like ads and mobile analytics
- OK disclosing coarse location information, more cautious with fine location
- OK disclosing fine location with SNS

Identifying a User's Privacy Profile

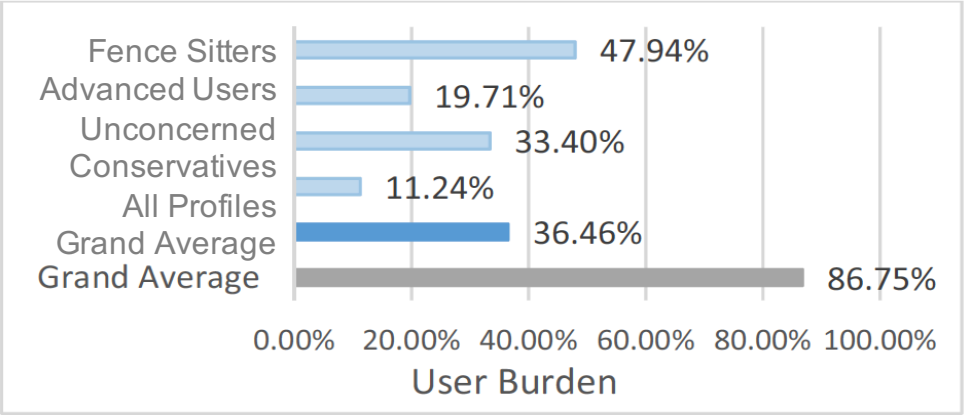
- Asking users a small set of questions (simulation)



Accuracy Estimates

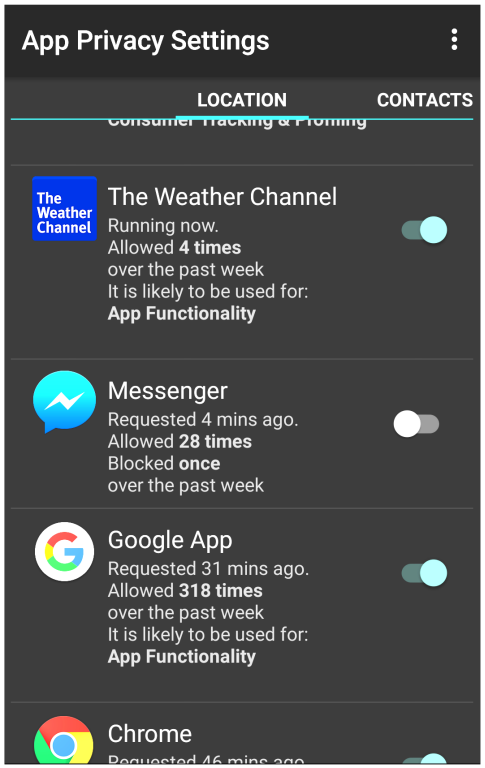


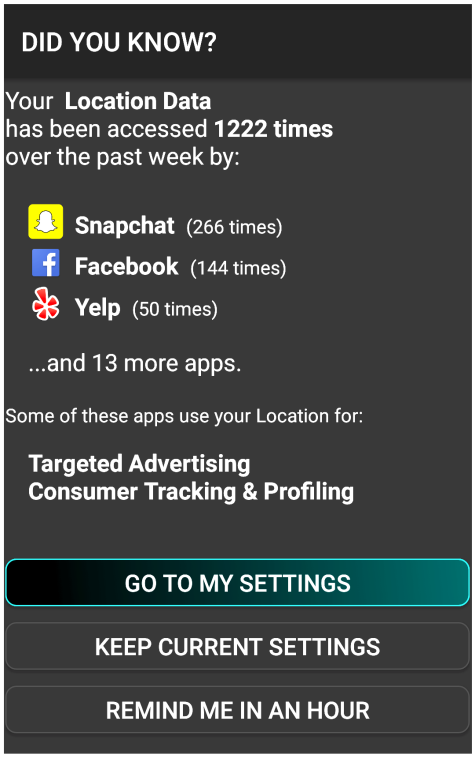
Accuracy:
One size fits all: 55.8%
4 Profiles: 79.4%



User Burden:
One size fits all: 86.8%
4 Profiles: 36.5%

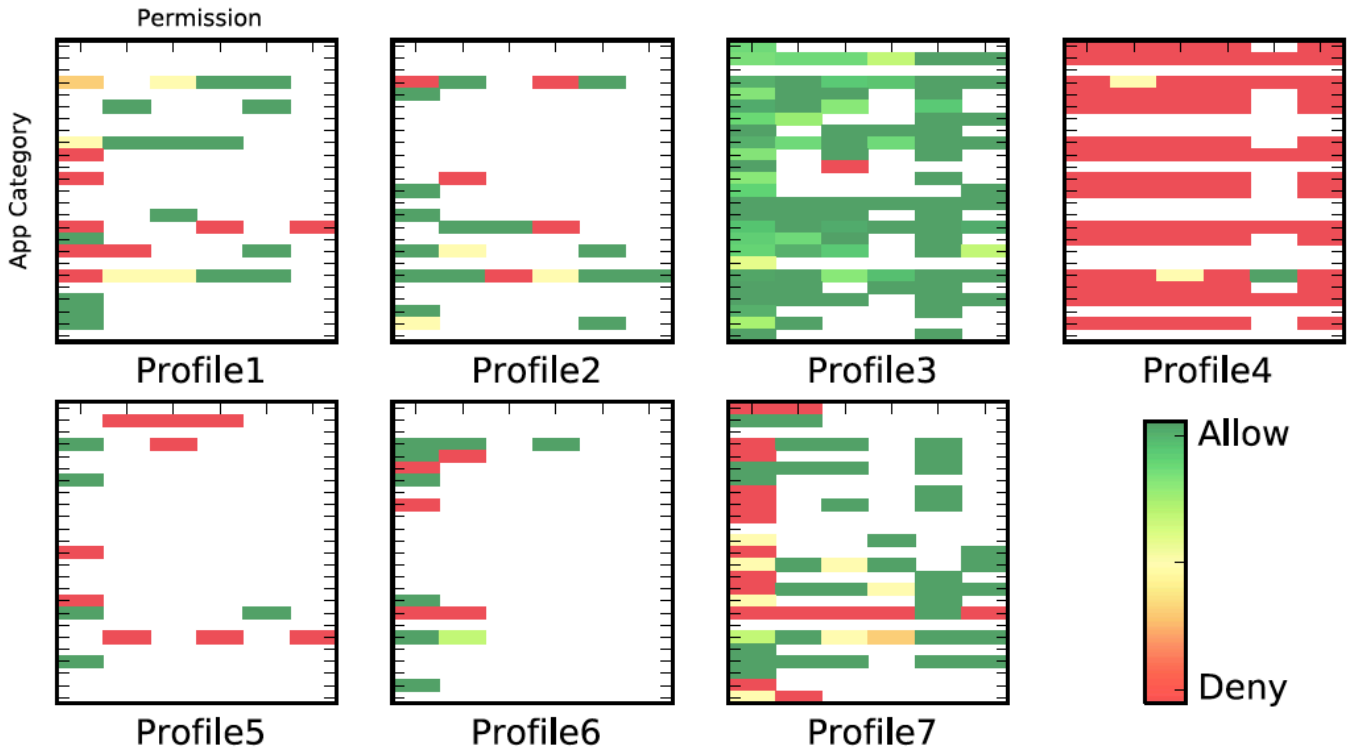
Learning People's Privacy Preferences with Nudges





"Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions", B. Liu, M. Schaarups Andersen, F. Schaub, H. Almuhimedi, S. Zhang, N. Sadeh, A. Acquisti, Y. Agarwal, Proc. of the USENIX Symposium on Usable Privacy and Security, SOUPS 2016, June 2016

Privacy Profiles – Hierarchical Clustering



- App categories along vertical axis; Permissions along horizontal axis
- Clustering based on triples for each user**: <app category, permission, purpose> - purpose can be obtained via static code analysis – similar to previous study**
- **Profile-based recommendations – using SVM**

Dialogue with Users: Profile Assignment & Setting Recommendations

These ***TRAVEL & LOCAL*** apps accessed your ***LOCATION 102 TIMES*** over the past 2 days:

- Maps
- GasBuddy
- San Francisco
- Yelp
- GrubHub
- Waze

In general, are you OK with ***TRAVEL & LOCAL*** apps accessing your ***LOCATION***?

YES

NO

Thank you! Based on your answers, we recommend restricting the following 11 app(s):

Click category to view/change recommendations

Deny 1 app(s) access to Calendar

Deny 9 app(s) access to Location

Facebook (50 times)	Allow	
News & Weather (0 times)	Deny	
Contacts+ (28 times)	Deny	
Messenger (16 times)	Allow	
Snapchat (84 times)	Deny	
Why deny? This Social app accesses your Location for App Functionality and Consumer Tracking & Profiling.		
QR Code Reader (0 times)	Deny	
Skype (0 times)	Deny	

Do you want to make these changes?

YES, DENY THE 8 APP(S) SELECTED

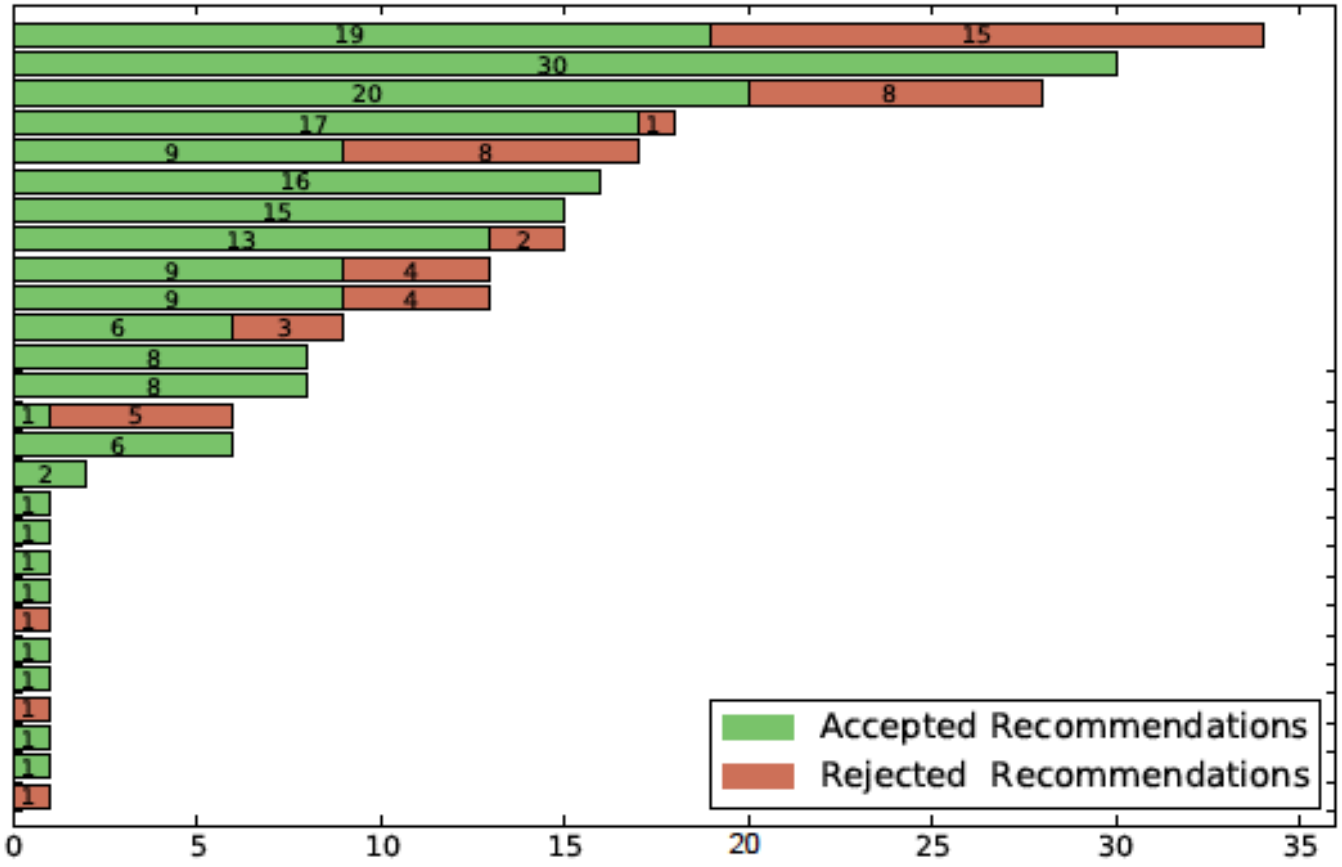
NO, DO NOT MAKE ANY CHANGES

Including explanation

Field Study: Evaluating the Recommendations

- **Recruited Android Users**: installed the privacy assistant on their actual Android phones; observed them as they used their phones and their apps as part of their regular activities
  - Day 1 and 2: collected usage data
  - Day 3: interaction with Privacy Assistant
- Starting on Day 4, participants were **subjected to nudges for an additional 6 days to see if they wanted to modify their settings**
- Total of 72 participants
  - **49 treatment condition – Privacy Assistant**
  - 22 control condition

Breakdown by User



Results (Treatment condition)

- **Users accepted 78.7% of Privacy Assistant's recommendations**
  - Could probably do even better with larger training set & more personalized learning
- Users showed great engagement as they received nudges for 6 days following interaction with the recommendations
  - A number of settings not covered by the recommendations were modified
- **Only 5.1% of accepted recommendations were modified over the 6 days**

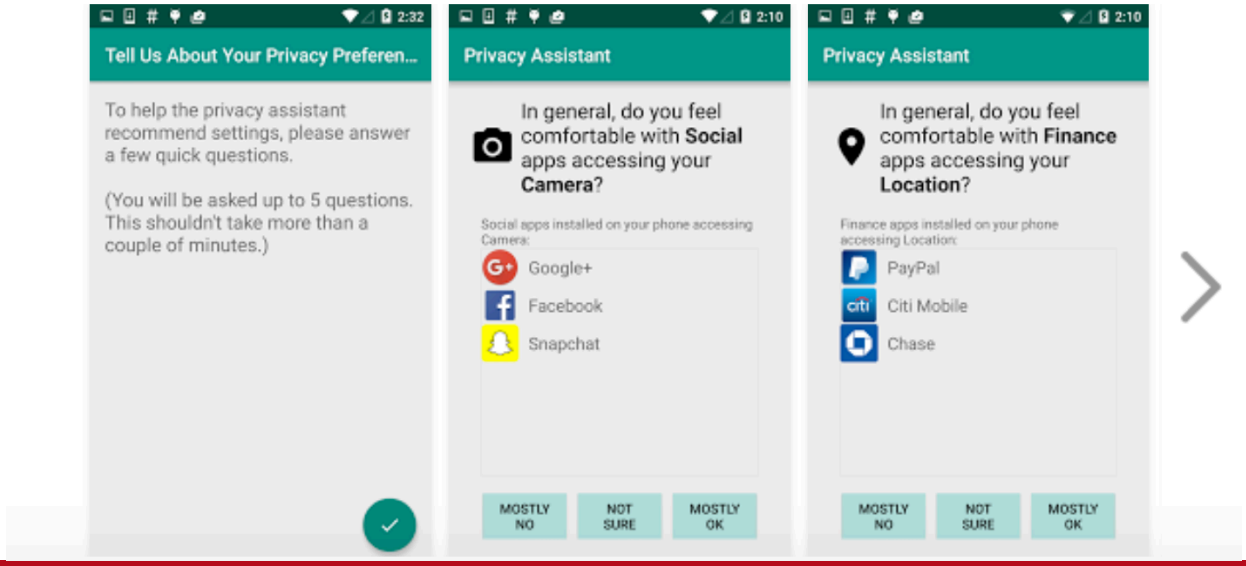
Mobile App Privacy Assistant*

[ROOT] Privacy Assistant

Mobile Commerce Lab @ Carnegie Mellon University Tools ★★★★☆ 4

Everyone

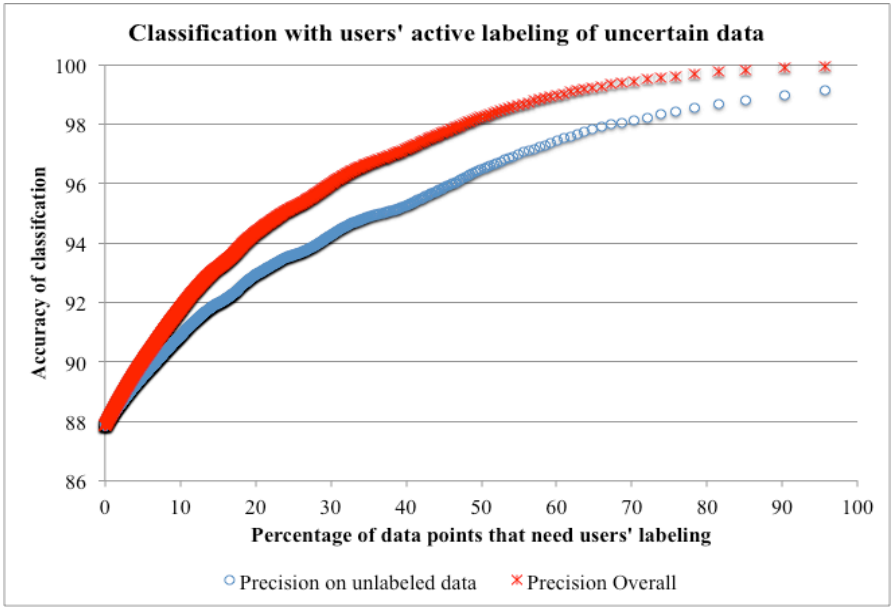
Add to Wishlist Install



* Patent pending

Mobile App Privacy Assistant Demo

Pure Prediction vs. Interactive Model



239K LBE users, 12K apps, 14.5M records

With more labeling of users, we can increase the accuracy of our predictions.

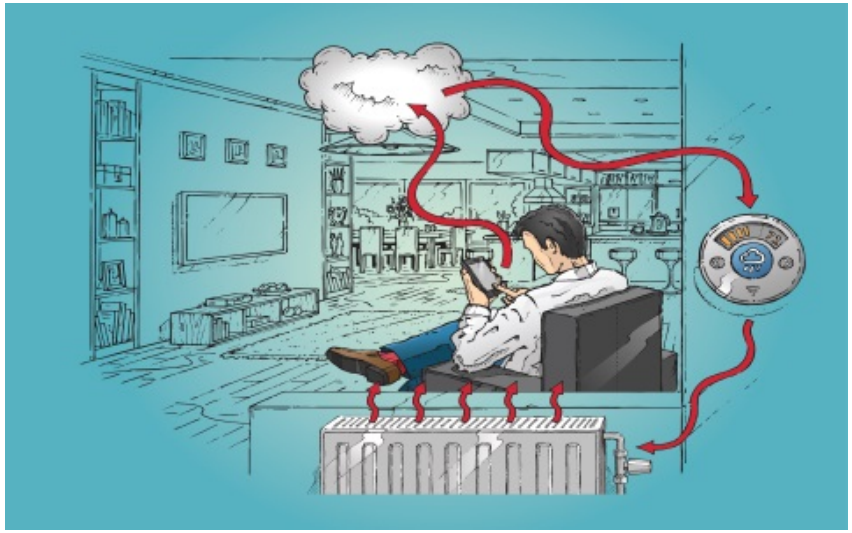
If users can label an additional 10% of their permission decisions, the **prediction accuracy will climb from 87.8% to 91.8%...and that's only 6 questions…**

At 20% (about 12 questions), accuracy climbs to 94%!

IoT Challenges

IoT entails additional challenges:

- No App Stores
- No (standardized) UI
- Often hidden, embedded
- More ways of collecting personal information
- Explosion in number of devices and services (scale)



Our Goals

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

Building an 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)

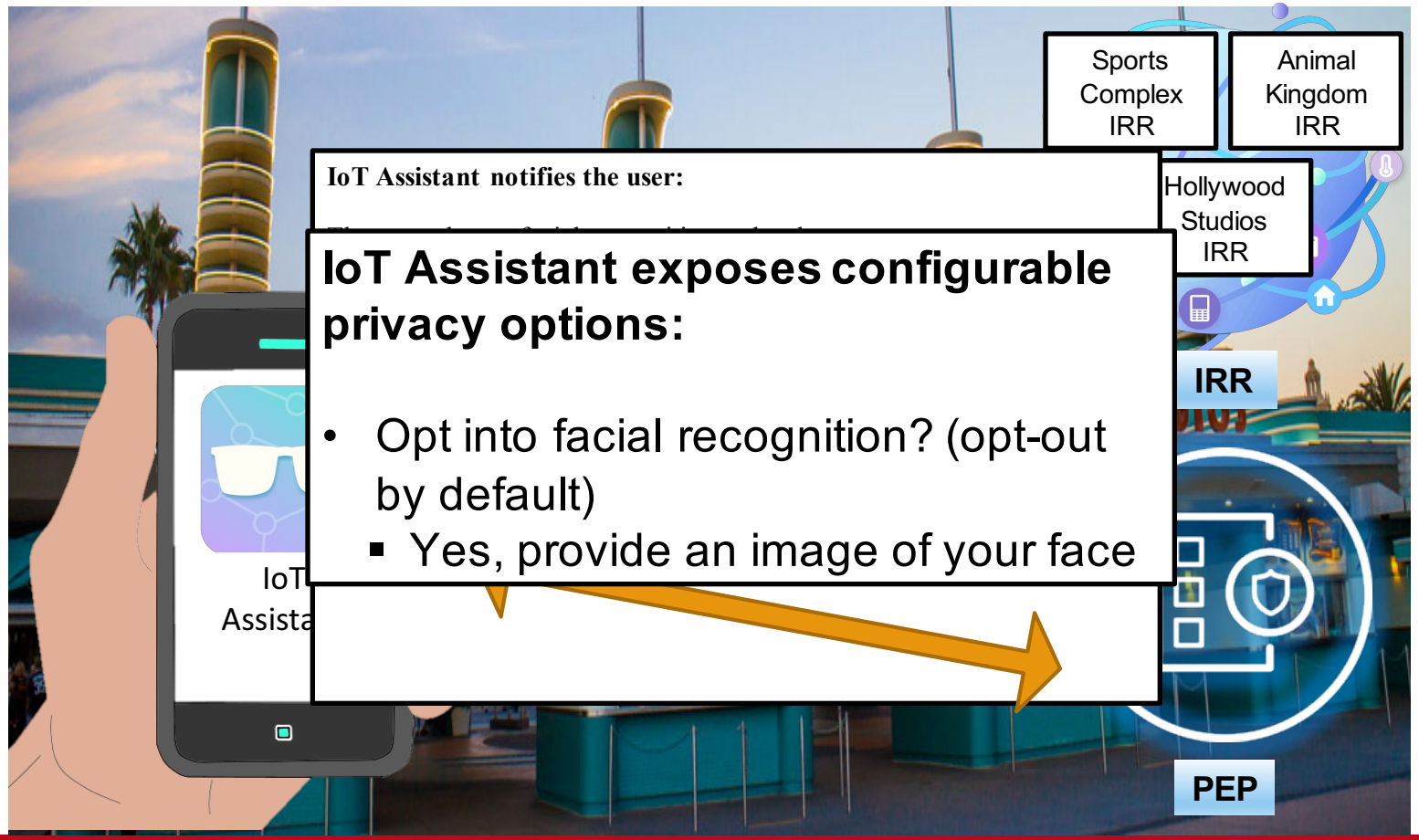
- Discovers IoT resources, their capabilities, and privacy practices (including any privacy settings)
- Learns user preferences; supports selective user notification, and semi-automated configuration of settings

Policy Enforcement Point (PEP)

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

* Patent pending

Theme Park Example



Key Features of the IRR

- Support for **multiple** (cloud based) **IRRs per location**
- Multiple **types of owners**, some IRRs more tightly managed than others (e.g. corporate, municipal, office, home)
- Multi-user support with **role based access control** (managing drafts and published resource descriptions)

IRR-BETA Administration Resource Management Martin Degeling

Support for multiple and geographically overlapping IRRs

About the IoT Resource Registry

source Registry is infrastructure that enables IoT service providers to connect with users. IoT-connected systems out collecting, storing, and processing sensitive data without ever being evident. Using information propagated e registry, we can empower choice by exposing IoT-connected systems and their privacy-relevant configuration sers can be notified about their potential encounters with IoT-connected systems in the physical world.

Using the Registry

IoT service and resource owners register their services' and resources' information, location, and configurable options. Users can then see what data collection efforts are occurring within the physical area of the registry's oversight. Users can browse and select configuration options relevant to their personal engagement with systems made discoverable by the registry. These options can include opting in or out, as well as other parameters that can be configured to suit their individual expectations of privacy.

CLICK TO LEARN MORE

IRR-BETA Administration Resource Management Martin Degeling

Administration and access control settings

About the IoT Res

The **IoT Resource Registr** enables IoT service providers to connect with users. IoT-connected systems may go about collecting, sensitive data without ever being evident. Using information propagated through the registry, we c exposing IoT-connected systems and their privacy-relevant configuration options. Users can be not ial encounters with IoT-connected systems in the physical world.

Using the Registry

IoT service and resource owners register their services' and resources' information, location, and configurable options. Users can then see what data collection efforts are occurring within the physical area of the registry's oversight. Users can browse and select configuration options relevant to their personal engagement with systems made discoverable by the registry. These options can include opting in or out, as well as other parameters that can be configured to suit their individual expectations of privacy.

CLICK TO LEARN MORE

IRR-BETA Administration Resource Management Martin Degeling

Multi User Support: Local, or Google-based account registration and authentication

About the IoT Resource Registry

The **IoT Resource Registry** is infrastructure that enables IoT service ... T-connected systems may go about collecting, storing, and processing sensitive data with ... mation propagated through the registry, we can empower choice by exposing IoT-connected systems and their privacy-relevant configuration options. Users can be notified about their potential encounters with IoT-connected systems in the physical world.

Using the Registry

IoT service and resource owners register their services' and resources' information, location, and configurable options. Users can then see what data collection efforts are occurring within the physical area of the registry's oversight. Users can browse and select configuration options relevant to their personal engagement with systems made discoverable by the registry. These options can include opting in or out, as well as other parameters that can be configured to suit their individual expectations of privacy.

CLICK TO LEARN MORE

View and Manage Resources

1. **IRR stores and retrieves information** about registered resources:
   - Location, capabilities, configuration options, privacy “short notice”
2. Add new devices **from scratch**, or use built-in **templates** for common devices
3. **Multi-User** Support

Overview of registered resources

IRR-BETA Administration Resource Management Martin Degeling

Search registered resources

Sort by

Below is a list of all the IoT resources that are registered to this IRR. Only those that are marked as "published" will be visible to IoT Assistants (the mobile client that resource users will use to discover and browse registered IoT resources).
You can register new resources by either starting from scratch, or select a template corresponding to a specifc type of IoT resource. Templates will fill in registration fields specific to that type of resource, allowing you to personalize the parameters specific to your deployment.

Select Template

REGISTER A NEW RESOURCE

Google Home

Google Home is a voice-activated speaker. It is powered by the Google Assistant. Ask it questions. Tell it to do things. And with support for multiple users, it can distinguish your voice from others in your home so you get a more personalized experience. It's your own Google, just for you.

Registered on Jul 3, 2017 by Martin Degeling

Is published

VIEW EDIT

CMU Urban Video Analytics Testbed

This installation is an initial prototype unit for the CMU Urban Video Analytics Testbed, which is an initiative involving the Intel Science and Technology Center for Visual Cloud Systems (ISTC-VCS) at CMU and the Metro 21 Initiative at CMU.

Registered on Jun 28, 2017 by Martin Degeling

Is published

iNoodle Zensor

This zensor detects how many people are waiting in line at iNoodle

Registered on Jun 28, 2017 by Martin Degeling

Is published

VIEW EDIT

FeelingSpector

The FeelingSpector computes the average mood of the users in front of them.

Registered on Jun 28, 2017 by Martin Degeling

Is published

VIEW EDIT

IRR-BETA Administration Resource Management Martin Degeling

Search registered resources

Sort by

Below is a list of all the IoT resources that are registered to this IRR. Only those that are marked as "published" will be visible to IoT Assistants (the mobile client that resource users will use to discover and browse registered IoT resources).
You can register new resources by either starting from scratch, or select a template corresponding to a specifc type of IoT resource. Templates will fill in registration fields specific to that type of resource, allowing you to personalize the parameters specific to your deployment.

Select Template

REGISTER A NEW RESOURCE

Administrators and resource owners control whether resources are published for others to discover

Google Home

Google Home is a voice-activated speaker. It is powered by the Google Assistant. Ask it questions. Tell it to do things. And with support for multiple users, it can distinguish your voice from others in your home so you get a more personalized experience. It's your own Google, just for you.

Registered on Jul 3, 2017 by Martin Degeling

Is published

VIEW EDIT

CMU Urban Video Analytics Testbed

This installation is an initial prototype unit for the CMU Urban Video Analytics Testbed, which is an initiative involving the Intel Science and Technology Center for Visual Cloud Systems (ISTC-VCS) at CMU and the Metro 21 Initiative at CMU.

Registered on Jun 28, 2017 by Martin Degeling

Is published

iNoodle Zensor

This zensor detects how many people are waiting in line at iNoodle

Registered on Jun 28, 2017 by Martin Degeling

Is published

VIEW EDIT

FeelingSpector

The FeelingSpector computes the average mood of the users in front of them.

Registered on Jun 28, 2017 by Martin Degeling

Is published

VIEW EDIT

IRR-BETA Administration Resource Management Martin Degeling

New resources can be defined using pre-filled fields from templates

Search registered resources

Sort by

Below is a list of all the IoT resources that are registered to this IRR. Only those that are marked as "published" will be visible to IoT Assistants (the mobile client that resource users will use to discover and browse registered IoT resources).
You can register new resources by either starting from scratch, or select a template corresponding to a specifc type of IoT resource. Templates will fill in registration fields specific to that type of resource, allowing you to personalize the parameters specific to your deployment.

Select Template

REGISTER A NEW RESOURCE

Google Home

Google Home is a voice-activated speaker. It is powered by the Google Assistant. Ask it questions. Tell it to do things. And with support for multiple users, it can distinguish your voice from others in your home so you get a more personalized experience. It's your own Google, just for you.

Registered on Jul 3, 2017 by Martin Degeling

Is published

VIEW EDIT

CMU Urban Video Analytics Testbed

This installation is an initial prototype unit for the CMU Urban Video Analytics Testbed, which is an initiative involving the Intel Science and Technology Center for Visual Cloud Systems (ISTC-VCS) at CMU and the Metro 21 Initiative at CMU.

Registered on Jun 28, 2017 by Martin Degeling

Is published

iNoodle Zensor

This zensor detects how many people are waiting in line at iNoodle

Registered on Jun 28, 2017 by Martin Degeling

Is published

VIEW EDIT

FeelingSpector

The FeelingSpector computes the average mood of the users in front of them.

Registered on Jun 28, 2017 by Martin Degeling

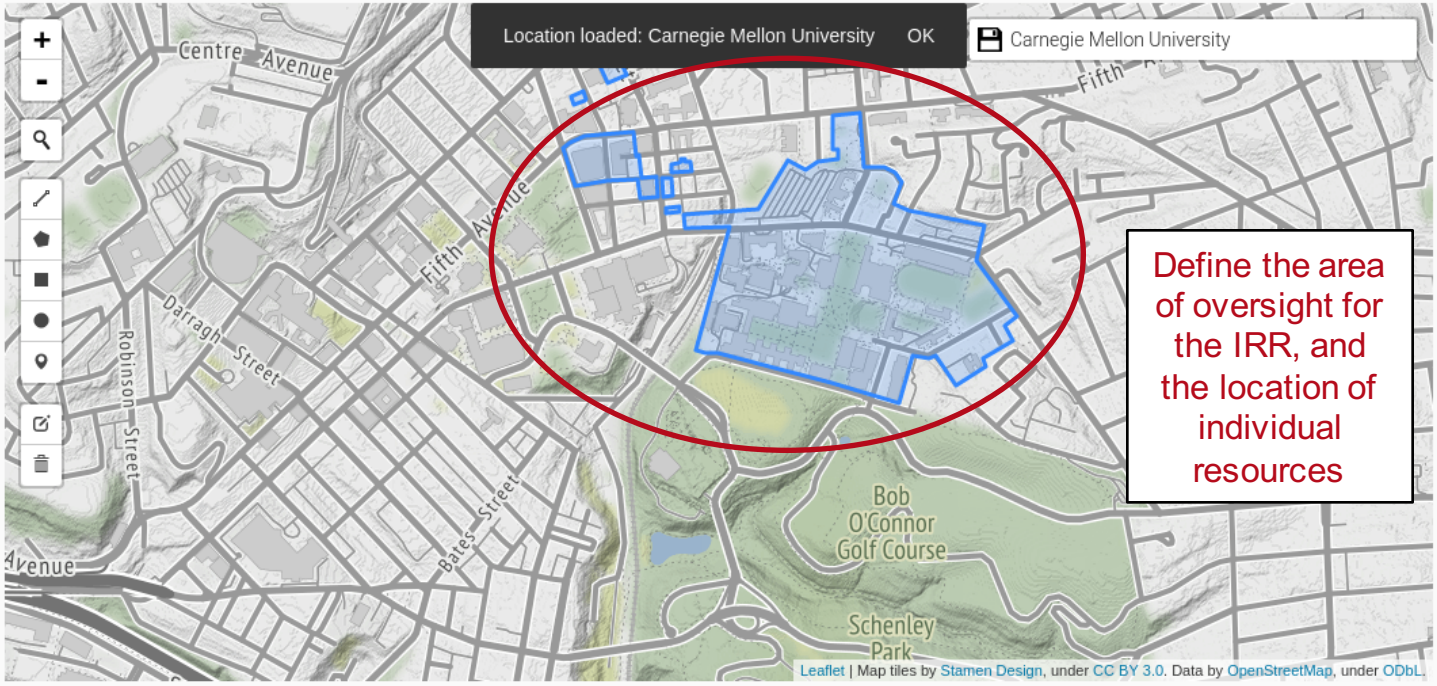
Is published

VIEW EDIT

Specify the Area of Oversight

1. **Specify the area the IRR oversees:**
   - This is the area or areas where resources will be advertised to IoTAs
2. **Specify locations for resources separately as you register them:**
   - Be as precise as you like; optionally, don’t specify a location

IRR-BETA Administration Resource Management Martin Degeling



Define the area of oversight for the IRR, and the location of individual resources

Owner Information

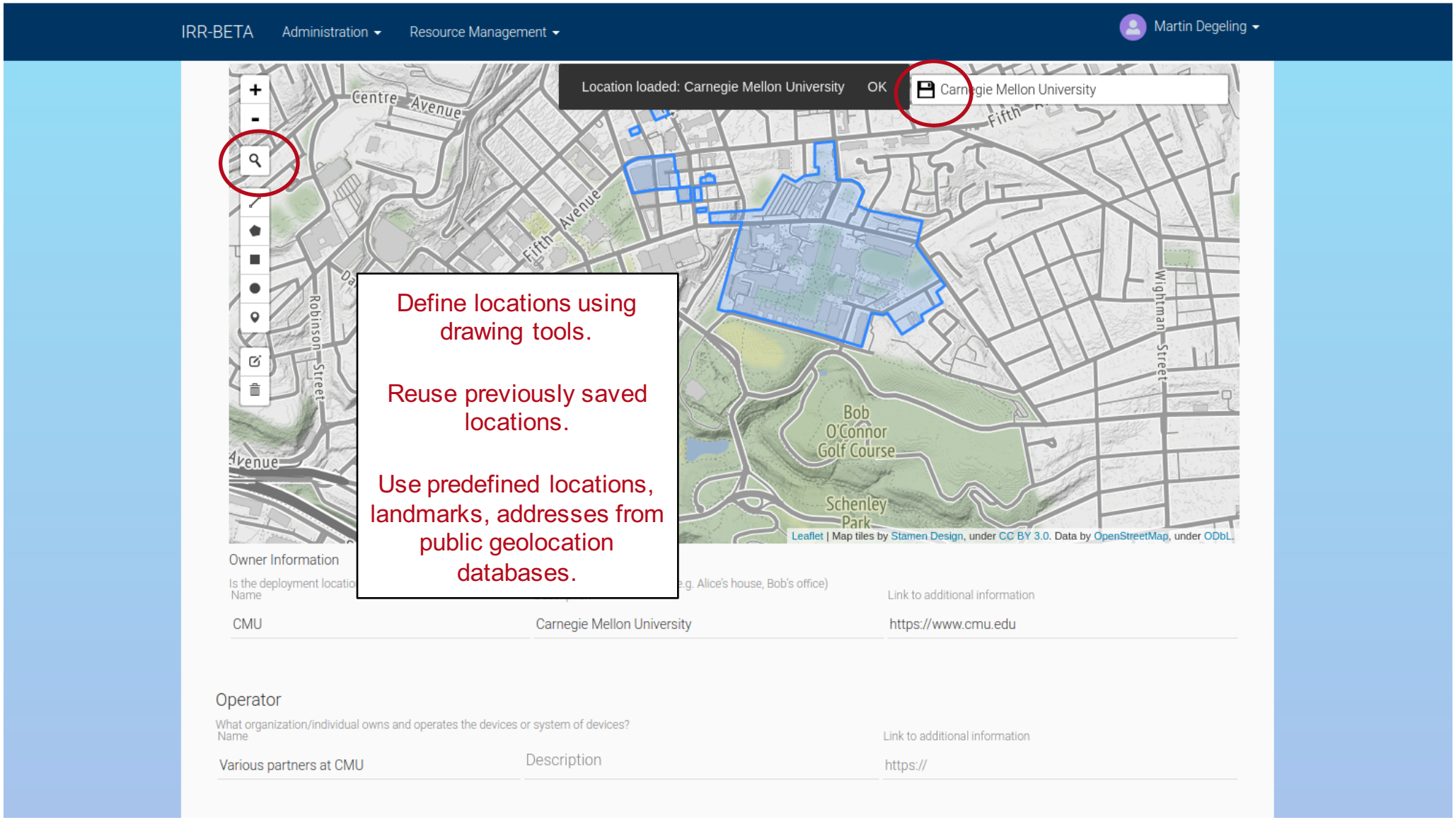
Is the deployment location owned by a business, government, public or privately owned? (e.g. Alice's house, Bob's office)

Name	Description	Link to additional information
CMU	Carnegie Mellon University	https://www.cmu.edu

Operator

What organization/individual owns and operates the devices or system of devices?

Name	Description	Link to additional information
Various partners at CMU		https://


IRR-BETA
Administration
Resource Management
Martin Degeling
Location loaded: Carnegie Mellon University
OK
Carnegie Mellon University
Centre Avenue
Fifth Avenue
Robinson Street
Wightman Street
Bob O'Connor Golf Course
Schenley Park
Leaflet | Map tiles by Stamen Design, under CC BY 3.0. Data by OpenStreetMap, under ODbL.
Define locations using drawing tools.
Reuse previously saved locations.
Use predefined locations, landmarks, addresses from public geolocation databases.
Owner Information
Name
CMU
Carnegie Mellon University
Link to additional information
https://www.cmu.edu
Operator
What organization/individual owns and operates the devices or system of devices?
Name
Various partners at CMU
Description
Link to additional information
https://

Specify Privacy Practices

- **Easy process to register new resources:**
  - Novel devices, sensors, etc. can be registered immediately
  - Informally specify resource capabilities
  - Generates “short notice” containing resource data practices
- **Small number of required fields**

IRR-BETA Administration Resource Management Martin Degeling

Basic Information | Context | Collected Data | Granularity | Purpose | Times and Retention | Shared With | Control Options

CANCEL SAVE

Basic Information

Name *
Amazon Echo

Link to general information about this resource
https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E

Description
Voice command device that performs a variety of functions

57 / 500

URI of an image that is displayed as logo or icon
https://images-na.ssl-images-amazon.com/images/I/41iz5Tw82IL._AC_US218_.jpg

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

Unique ID (e.g. edu.cmu.iot) *
echo

Type of Resource *
Data Collection

NEXT

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

Fields Based on Policy Schema

- Machine-readable policy schema
- Can represent various types of information on privacy practices for users, e.g.
  - Location
  - Granularity of data collection
  - Retention
  - Purpose
  - Sharing

```
{
  "id": "http://www.privacyassistant.org/static/schema/1.4.json",
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "IoT Privacy Policy",
  "description": "The document itself is made up of at least one collection instance. Multiple collection instances r
  "type": "object",
  "properties": {
    "language_version": {
      "description": "The version of the language used",
      "type": "string"
    },
    "resource": {
      "description": "The list of IoT resources in that place",
      "$ref": "#/definitions/resourceType"
    }
  },
  "required": [
    "resource",
    "language_version"
  ],
  "definitions": {
    "resourceType": {
      "id": "#resourceType",
      "description": "There are different attributes that will be specified in a privacy policy. Each attribute will
      "properties": {
        "info": {
          "description": "Summary general information about the data collection",
          "allOf": [
            {
              "$ref": "#/definitions/informationType"
            },
            {
              "properties": {
                "id": {
                  "type": "string"
                },
                "version": {
                  "type": "number"
                },
                "privacy_policy": {
                  "type": "string",
                  "format": "url"
                },
                "logo_uri": {
                  "description": "URI of an image that is displayed as logo or icon",
                  "type": "string",
```

Pappachan et al. “Towards Expressing Privacy Requirements in Smart Buildings.” (IoTCA 2017)

IRR-BETA Administration Resource Management Martin Degeling

Basic Information | Context | Collected Data | Granularity | Purpose | Times and Retention | Shared With | Control Options

CANCEL SAVE

Basic Information

Name *
Amazon Echo

Link to general information about this resource
https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E

Description
Voice command device that performs a variety of functions

URI of an image that is displayed as logo or icon
https://images-na.ssl-images-amazon.com/images/I/41iz5Tw82IL._AC_US218_.jpg

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

Unique ID (e.g. edu.cmu.iot) *
echo

Type of Resource *
Data Collection

NEXT

Start simple, add more details later…

Only a few fields are required to create a valid registry entry

IRR-BETA Administration Resource Management Martin Degeling

Register a New Resource

Basic Information | Context | Collected Data | Granularity | Purpose | Times and Retention | Shared With | Control Options

CANCEL SAVE

Add any custom control options of your resource that are not related to any of the section you have previously specified.

Control Options

1. Edit your Echo settings

PREVIOUS

Define how users interact or configure (using their IoT Assistant) resources you register on this IRR.

SAVE Share the template

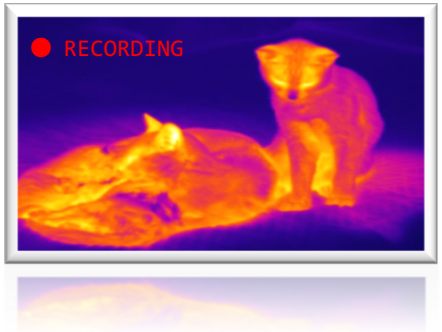
Click to enable manual mode

Enabling Privacy Choice

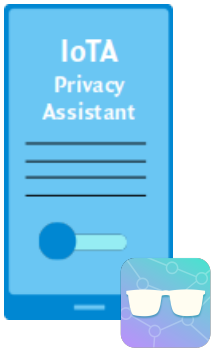
1. **Define privacy options for resources** that end-users can individually configure
2. **Specify control** endpoints (i.e. REST, APIs) for resources' configurable options
3. **Requests are authenticated**

Multi-User Home Setup Scenario

1. Alice is setting up a new internet enabled thermal camera in her home, to keep an eye on her pets.



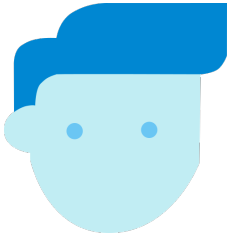
5. Bob's IoTA exposes the option to disable Alice's camera while he is there.



2. Alice registers the camera with her home IRR to inform visitors about it, and let them control recording.

IoT Resource Registry

3. Bob visits Alice.



4. Bob's IoTA discovers Alice's IRR and its policies. Bob's IoTA knows that he prefers *not* to be recorded on video in private spaces.

IoT Assistant: Functionality

1. The **IoTA connects users with relevant IRR(s)** based on their location
2. **Shows list of registered resources** under the oversight of connected IRRs

IoT Assistant: Key Features

1. **Informs user about privacy practices**
2. **Exposes privacy settings** that may (or may not) be available for user to configure

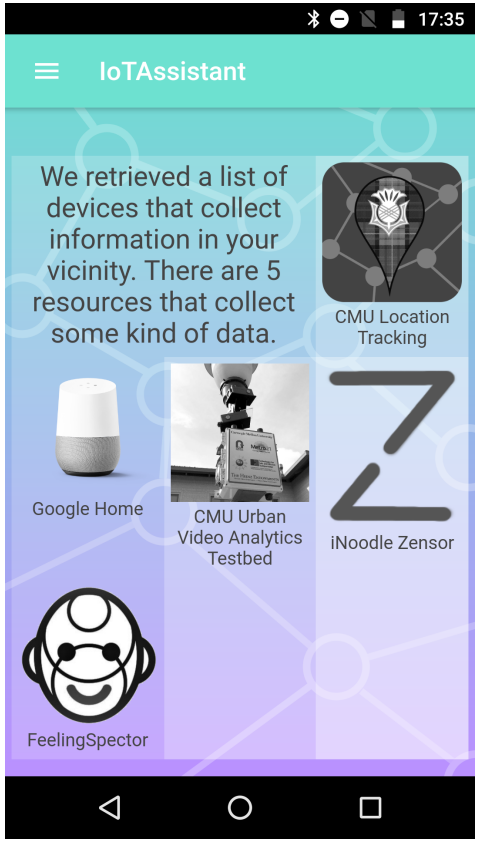
In the future…

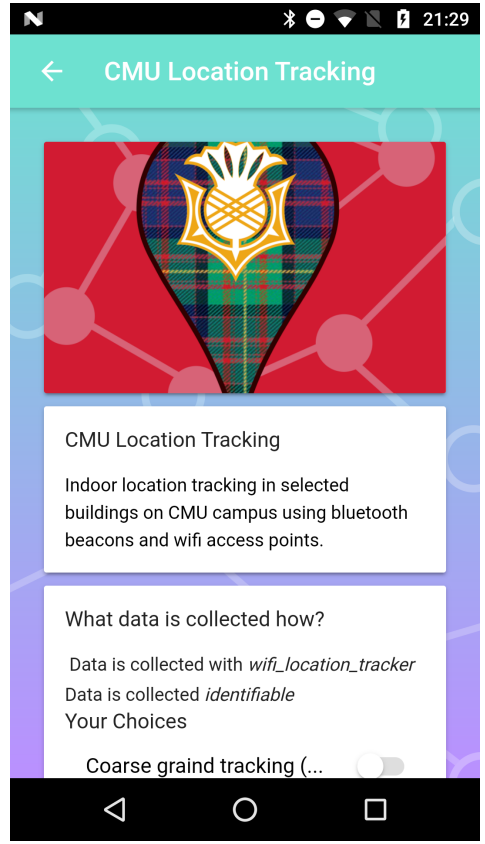
Semi-automatically leverage user privacy preferences:

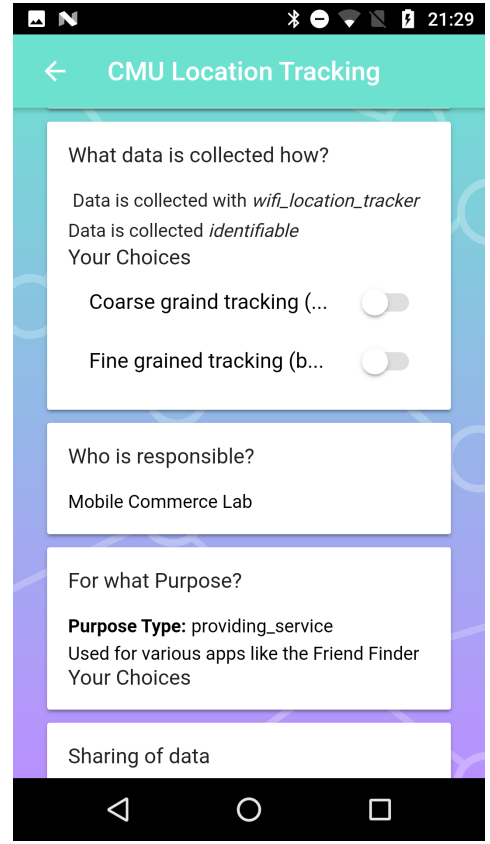
- **What to notify the user about?**
- **When to notify (including how often)?**
- **How to notify (e.g. buzzing, vibrating, flashing, etc.)?**

Naeini et al. "Privacy Expectations and Preferences in an IoT World." SOUPS 2017

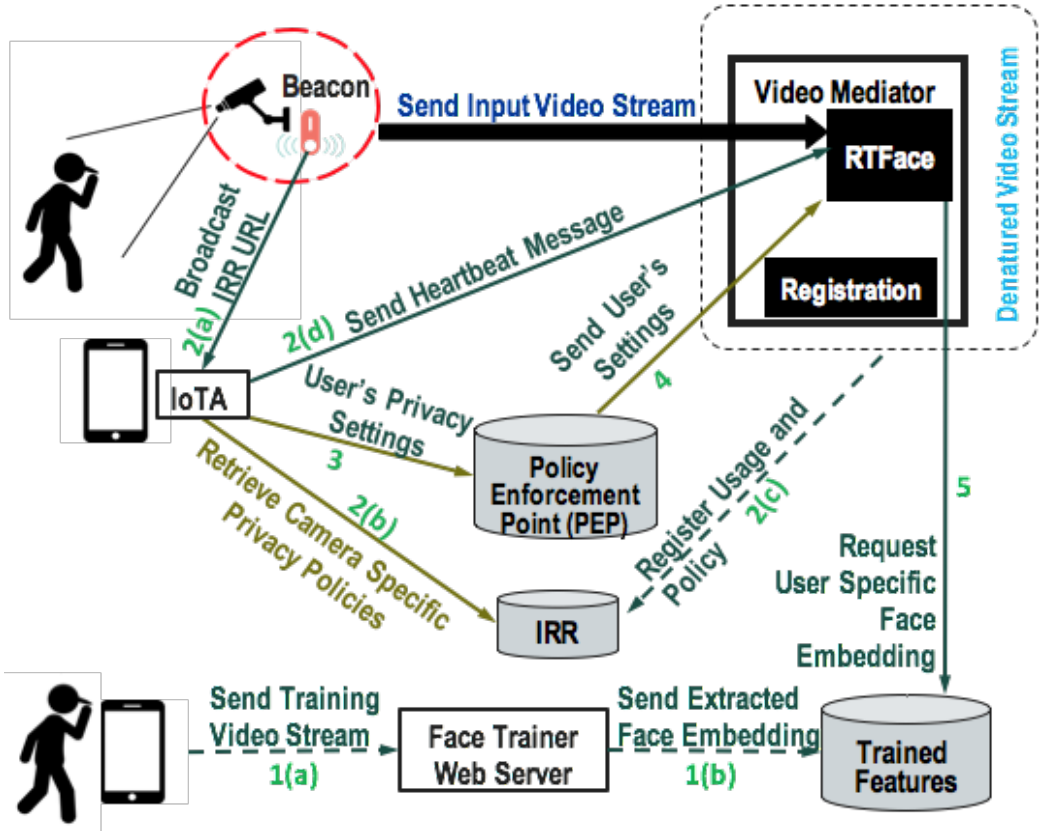
IoT Assistant







Example: Privacy-aware Video Streaming

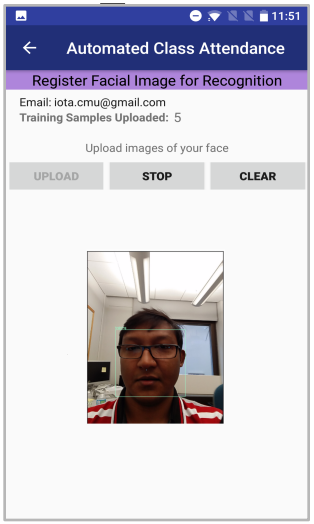


Obfuscates faces being recorded in video streams in real-time.

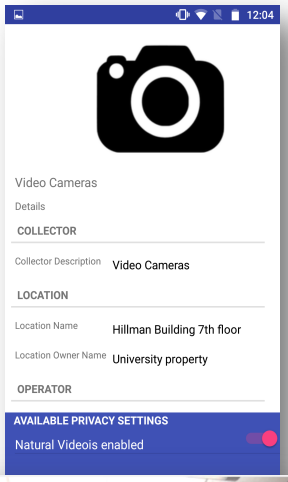
Wang et al., "A Scalable and Privacy-Aware IoT Service for Live Video Analytics", MMSys 2017 (**Best Paper Award**)
Das, Anupam et a. "A Privacy-Aware Infrastructure for Using Facial Recognition." (CV-COPS 2017)

Automated Attendance Tracker

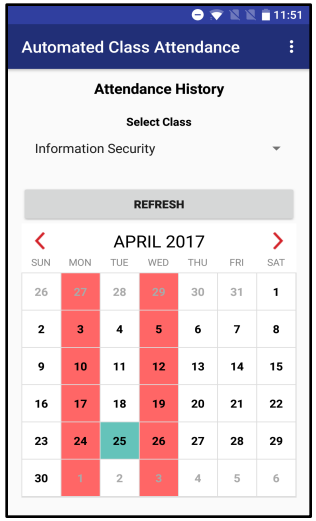
Train Facial Features



Control Opt-in



Monitor Class



Live Video Stream

Demo

Discussion: Possible Uses of IoT Privacy Infrastructure

- Is this something that you could see your company/university deploy at some point?
- Is this something that you could see a use for in your home?
- Is this something that you wish your city or your mall would deploy?
- Is this something that you could use as a researcher/developer?
- What features would you be most likely to use/want?

Session III Recap

- People's privacy preferences are complex and malleable
- Explosion in permission settings
- Opportunity to learn people's privacy preferences – not just to help users configure settings but also to learn when to notify users (situations, frequency, manner)
- Nudges can be used to increase to fidelity of permission settings
- Profile-based mobile app permission assistant
- IoT Infrastructure for IoT privacy assistant – incl. registries

More Information?

- See our Poster tonight!
- Ask one of us for a demo while at the conference

- The **Privacy Assistant Project** involves a collaboration with a number of individuals.
- See **privacyassistant.org** for additional details incl. lists of collaborators, publications, sponsors and recent news
- Subscribe to our mailing list to stay up to date - https://www.privacyassistant.org/contact