Privacy in IoT-Based Smartspaces

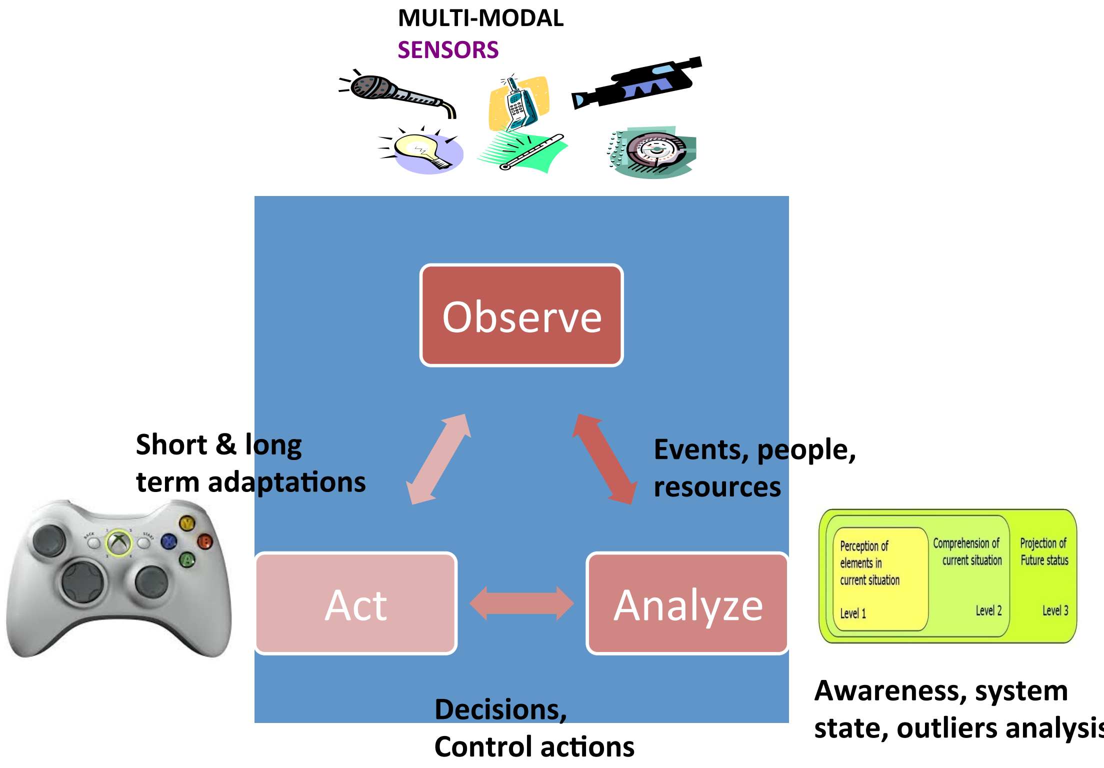
CalPlug Workshop, Calit2 UCI

May 12, 2016

Nalini Venkatasubramanian
Department of Computer Science &
Center for Emergency Response Technologies
University of CA, Irvine

Internet of Things

Systems that empower everyday physical devices to connect to the internet and to send & receive messages



MULTI-MODAL
SENSORS

Observe

Act

Analyze

Short & long
term adaptations

Events, people,
resources

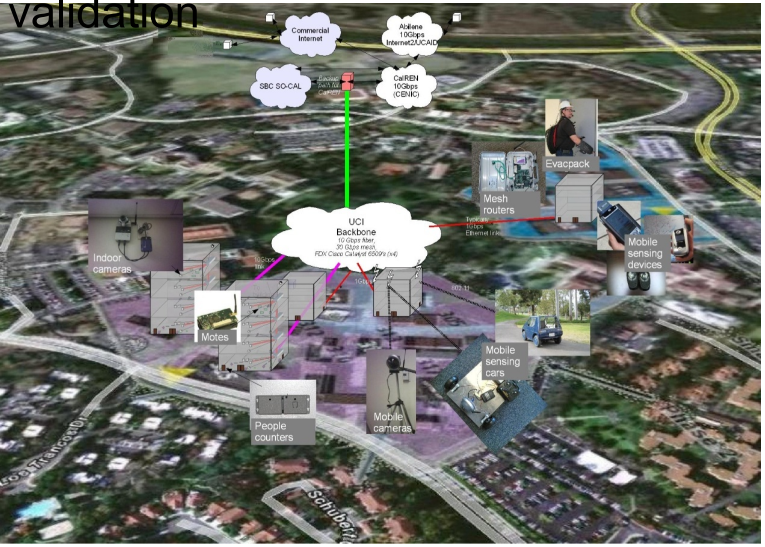
Decisions,
Control actions

Awareness, system
state, outliers analysis

- **Over 25 billion devices connected at the end of this year**
- **Expected to reach a trillion by next decade**
- **Mobile traffic to exceed 15 exabytes of data by each month by 2018**

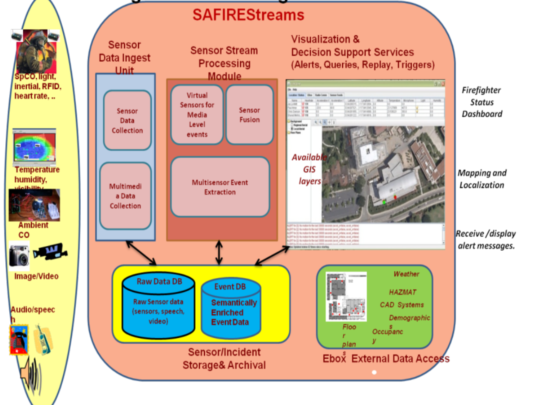
Sample SmartSpaces and Derivative Artifacts

Responsphere - A Campus-wide infrastructure to instrument, monitor, disaster drills & technology validation



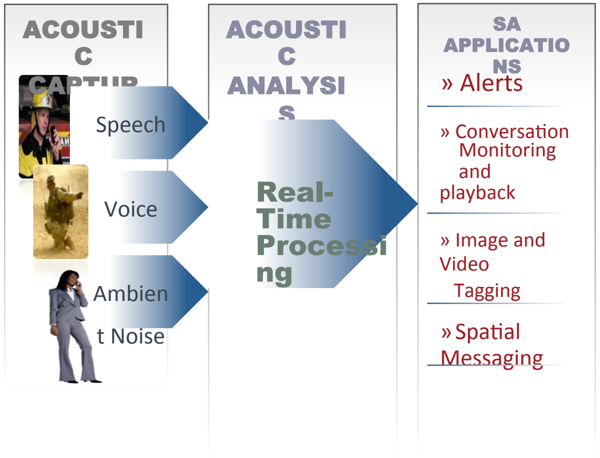
SAFIRE – Situational awareness for fire incident command

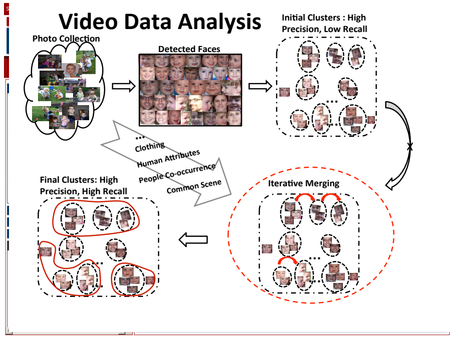
The SAFIRE (Situational awareness for Firefighters) Project: Sensing -> Sensemaking for the Fire Practice

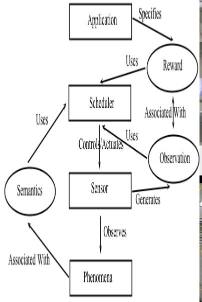

SAFIREStreams
SpCO, light, inertial, RFID, heart rate, ..
Temperature humidity, visibility
Ambient CO
Image/Video
Audio/speech
Sensor Data Ingest Unit
Sensor Data Collection
Multimedia Data Collection
Sensor Stream Processing Module
Virtual Sensors for Media Level events
Sensor Fusion
Multisensor Event Extraction
Visualization & Decision Support Services (Alerts, Queries, Replay, Triggers)
Available GIS layers
Firefighter Status Dashboard
Mapping and Localization
Receive /display alert messages.
Raw Data DB
Raw Sensor data (sensors, speech, video)
Event DB
Semantically Enriched Event Data
Sensor/Incident Storage& Archival
Weather
HAZMAT
CAD Systems
Demographics
Floor plans
Occupancy
Ebox External Data Access

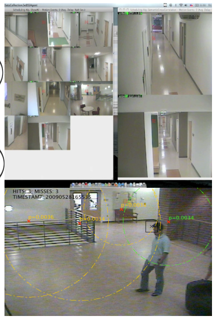
Goal: Reliable Timely SA over Unpredictable Infrastructure

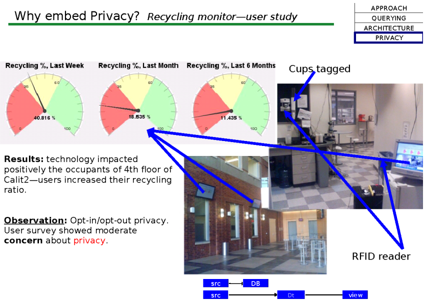
OpsTalk– Speech based awareness & alerting system for soldiers on the field









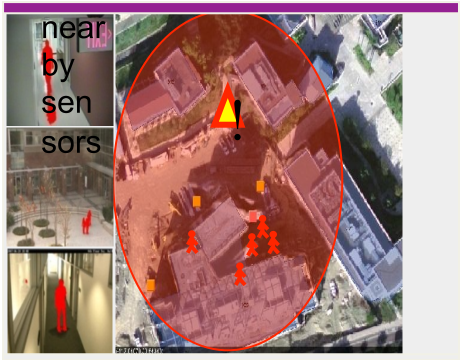


Why embed Privacy? *Recycling monitor—user study*

APPROACH
QUERYING
ARCHITECTURE
PRIVACY

Results: technology impacted positively the occupants of 4th floor of Calit2—users increased their recycling ratio.

<u>Observation</u>: Opt-in/opt-out privacy. User survey showed moderate **concern** about privacy.



Adaptive Semantic Sensor Data Collection and Analytics (Video/Images)

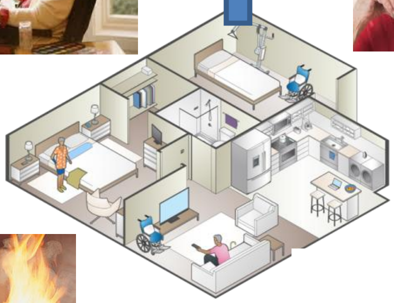
Calit2 Recycling Monitor

Privacy Preserving Surveillance

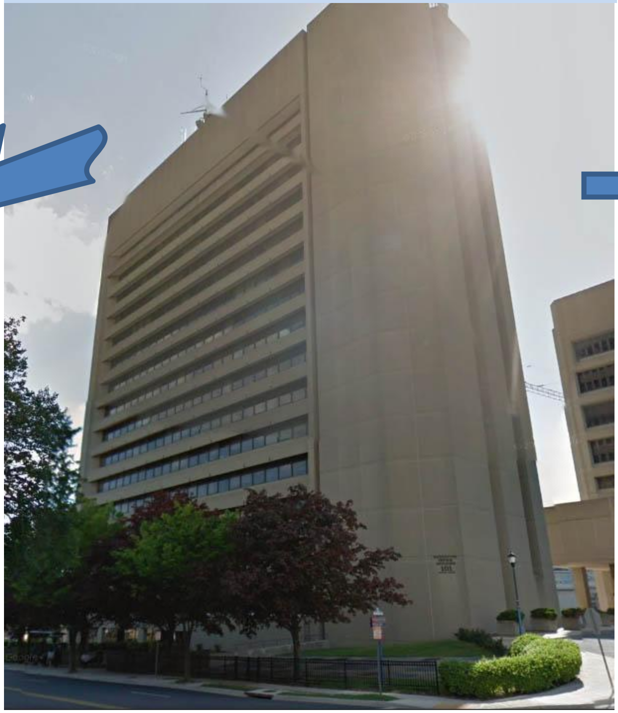
SCALE (Smart Community Awareness and Alerting)
A SmartAmerica Project – Democratizing IoT

Extending the Internet of Things to Everyone: Residents of an affordable housing complex who cannot otherwise afford broadband are given smart community sensors. A resident, possibly elderly, is in distress and the sensor sends a signal to the nearest base station.

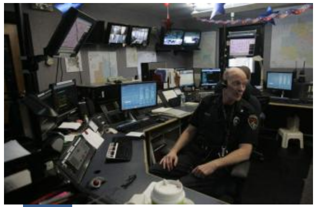
MHP
MONTGOMERY HOUSING PARTNERSHIP



County Facility Equipped with Antenna



Cloud-based public safety awareness and alert system



Dispatch Center

Emergency validated via mobile device; alert is sent to the dispatch center and a first response unit is sent to the resident in distress.

Within minutes first responders arrive without any need for manual action by the person in distress

Building Management Systems (BMS)

Cyber-physical systems that are used to *manage buildings and services* provided in that er

New opportunity, new trend

MIXING building data with individual centric data

Leads to (unanticipated) privacy challenges

- Fire and seismic safety
- Water Supply & sewage
- Special needs (e.g. hospitals, stadiums)

HVAC Maintenance
Fire Detection
Environmental Control
Mechanical Maintenance
Asset Locator
Enterprise Systems Integration
Water Management
Energy Information Management
On-Site Technical Service

Risks in the context of IoT…

BMS (& other IoT applications) provide unprecedented benefits, but…

They come at the cost of:

- **Security risks**
  - Devices increase the attack surface, introduce new vulnerabilities, introduce new type of attacks.
- **Privacy risks**
  - Highly granular sensors data may capture information about individuals, their location, habits, health status, religious affiliation, behavior, likes/dislikes, …

Things that people often consider private!

TIPPERS *(Testbed for IoT-based Privacy-Preserving PERvasive Spaces)* - *A DARPA Brandeis Project*

Sharad Mehrotra, Nalini Venkatasubramanian, Alfred Kobsa

University of California Irvine

Raj Rajgopalan

Honeywell Research

+ a large team of TIPPERS researchers & developers at UCI CS + Calit2 + Honeywell

TIPPERS Testbed Overview

Physical building with heterogeneous devices, real people and real activities

- Bren Hall -- a relatively large shared deeply sensed space

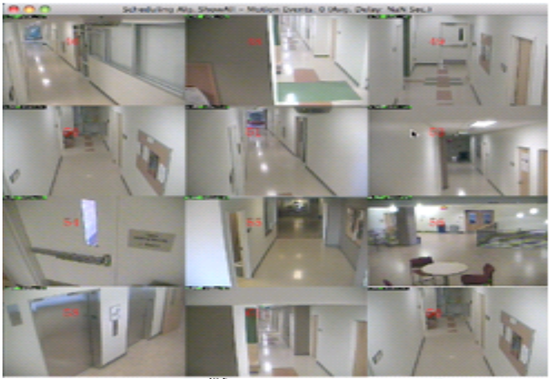
An industrial strength building management system

- Adaptive flexible interfaces that support mechanisms to retrofit privacy technologies.

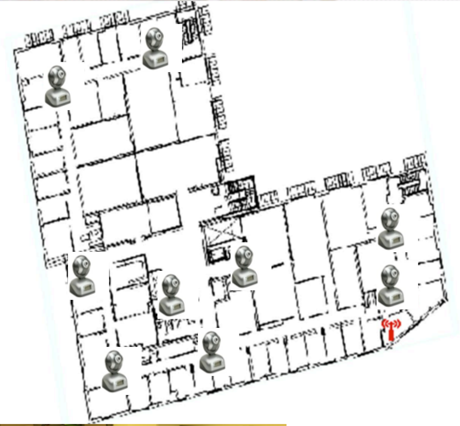
An experimental research system with plug-n-play potential to support privacy technologies

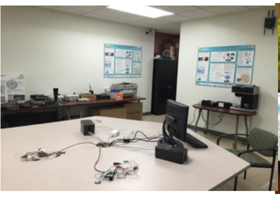
- Designed ground up to embody ***"privacy by design"*** principle.
- Customizable to multiple usage scenarios.

Bren Hall: TIPPERS Instrumented Building



- 6 Story Building
- **90,000 sq. ft classroon**
- 125 Faculty Offices
- **90 Research Labs**
- Lecture Halls
- **Departmental Offices**

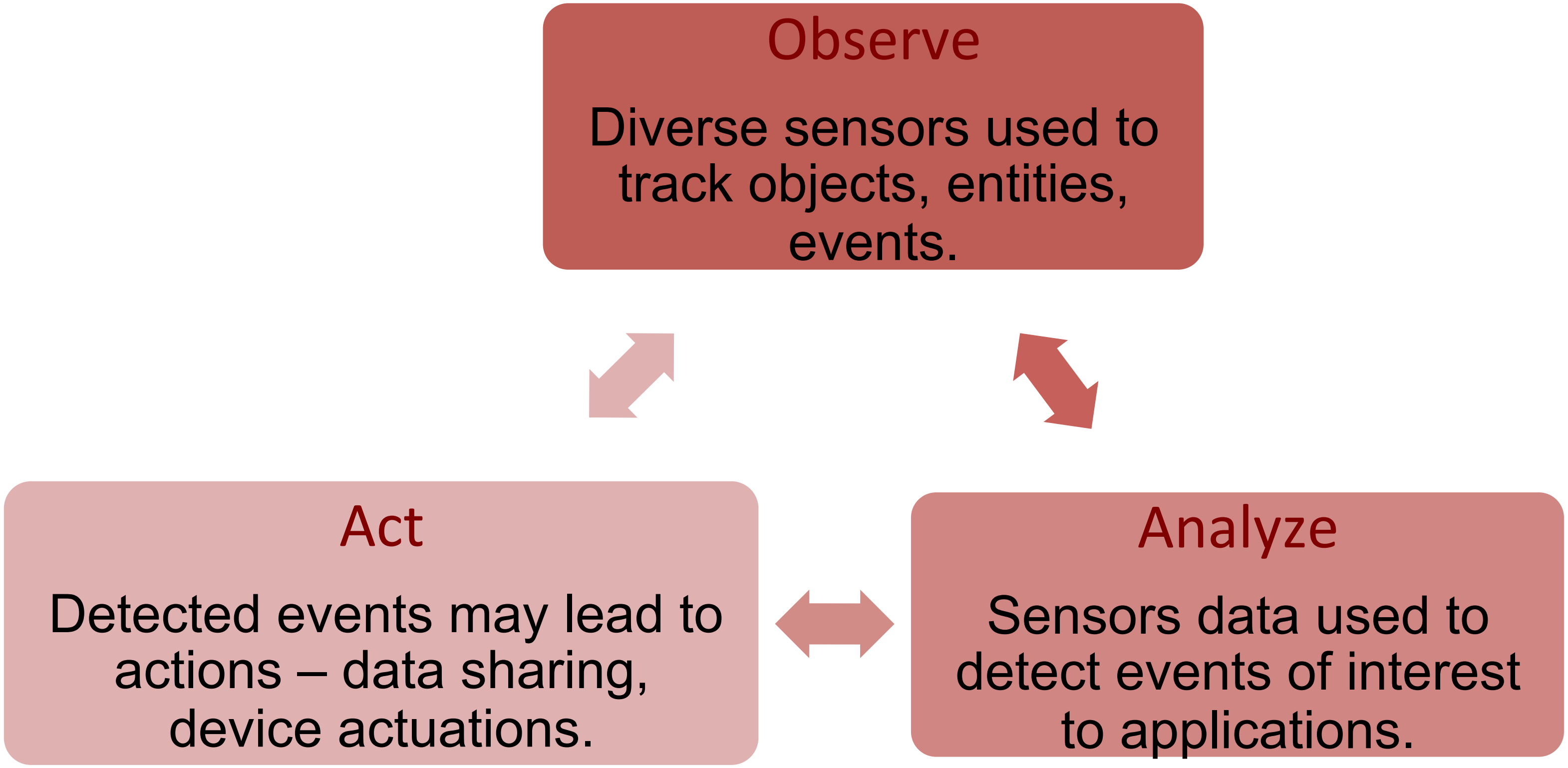




Diverse set of sensors installed

Data Flow & Associated Risks

Data flow in IoT systems



Observe

Diverse sensors used to track objects, entities, events.

Analyze

Sensors data used to detect events of interest to applications.

Act

Detected events may lead to actions – data sharing, device actuations.

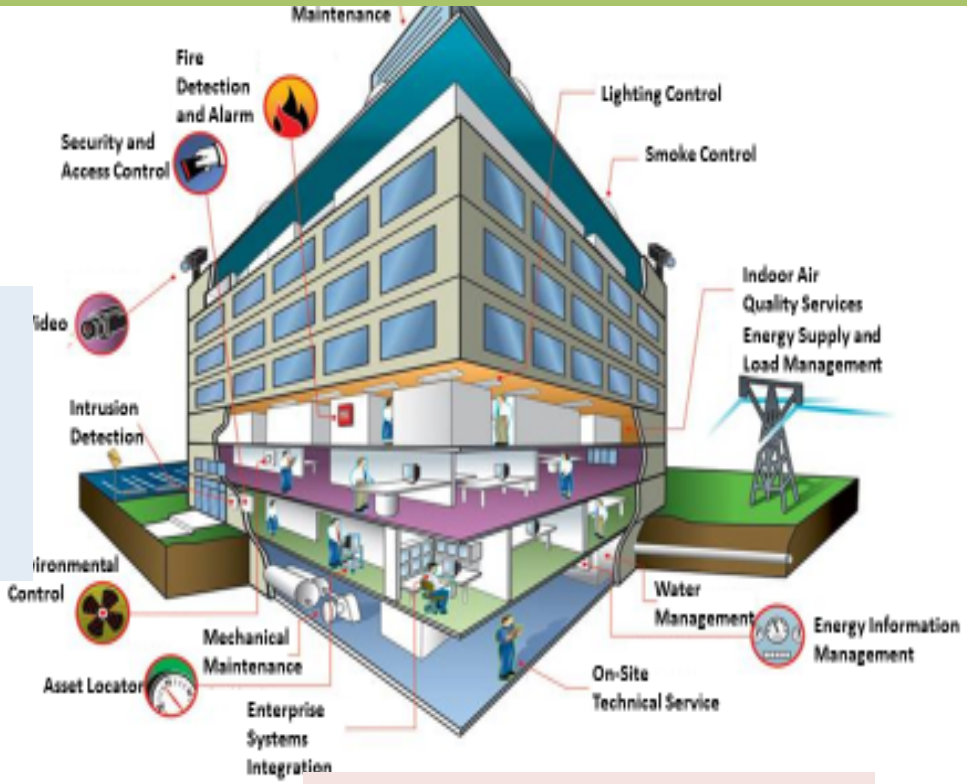
Each step poses disclosure risks - depends upon underlying trust model

Privacy and Utility
New Building Management Systems (BMS + IoT)

MIXING building data with individual centric data

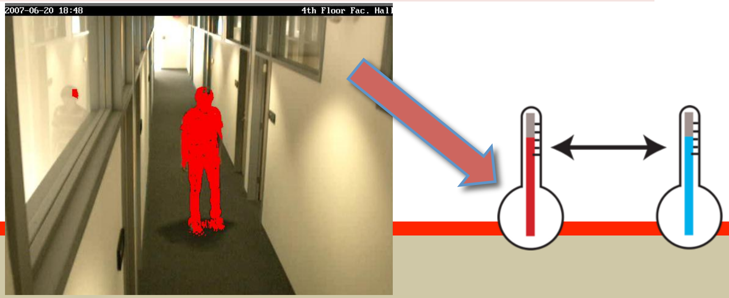
Improved management

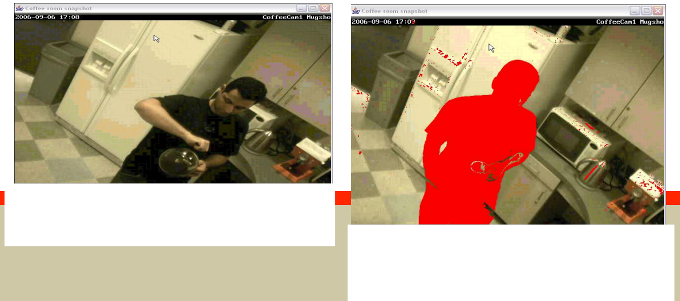
Enhanced services


Maintenance
Fire Detection and Alarm
Security and Access Control
Lighting Control
Smoke Control
ideo
Indoor Air Quality Services
Energy Supply and Load Management
Intrusion Detection
ironmental Control
Water Management
Energy Information Management
Mechanical Maintenance
Asset Locator
On-Site Technical Service
Enterprise Systems Integration

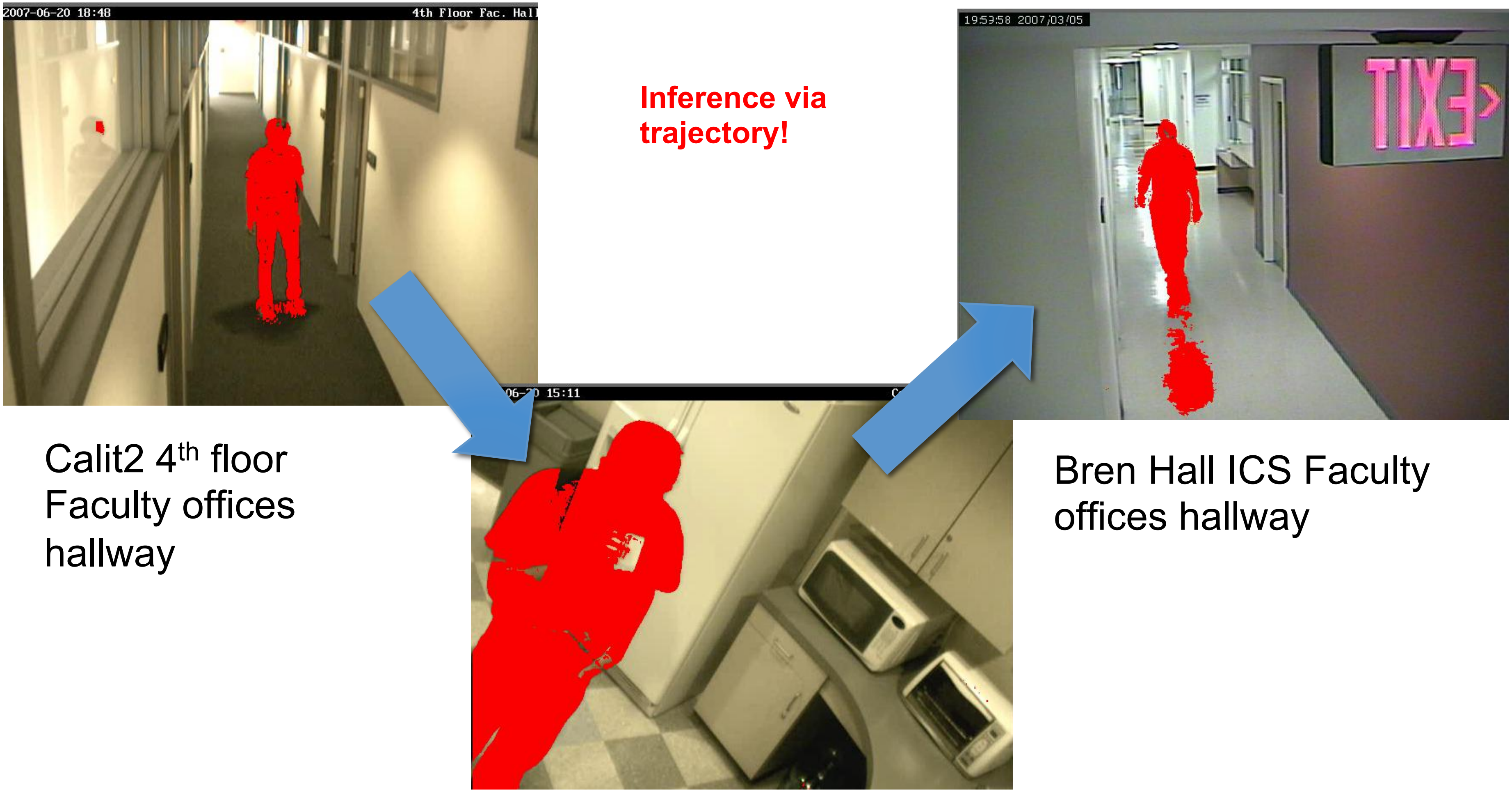
Change in HVAC as a result of a person entering a room may allow observer to infer the identity of the person.

Single Sensor discloses identity





Inference from Sensor Data [ACM MM 2006]



Inference via trajectory!

Calit2 4th floor Faculty offices hallway

Bren Hall ICS Faculty offices hallway

Calit2 4th floor kitchen

Inference via Event Detection [PERCOM 2009]

Consider two events

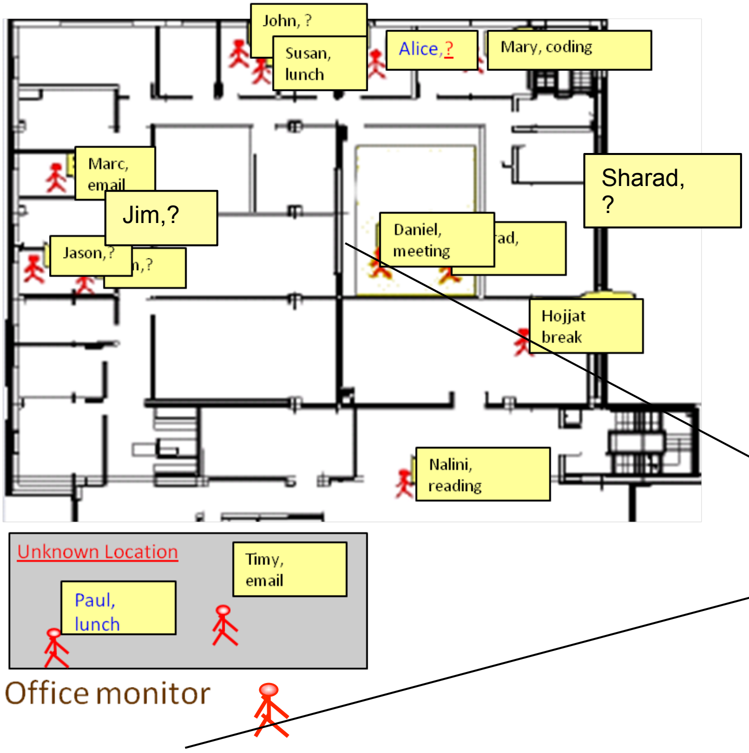
- E1: identify when a Calit2 researcher enters space A
- E2: identify when a TIPPERS enters the space B

Knowledge:

- If we know E1 detected → 1 out of ~30
- If we know E2 detected →1 out of ~20
- If we know some event was detected (not which one) →1 out of ~47
- If we know both events detected → 1 out of ~3!
- Replace Calit2 researcher by CalPlug Researcher → we know it is **Sergio**!!!

Knowledge about the system's state can lead to disclosure

Inference from Action [ACM Middleware 2009]



Office monitor

Public knowledge:

“Alice and Paul always have lunch together.”

+ ➡

→ Alice is having lunch

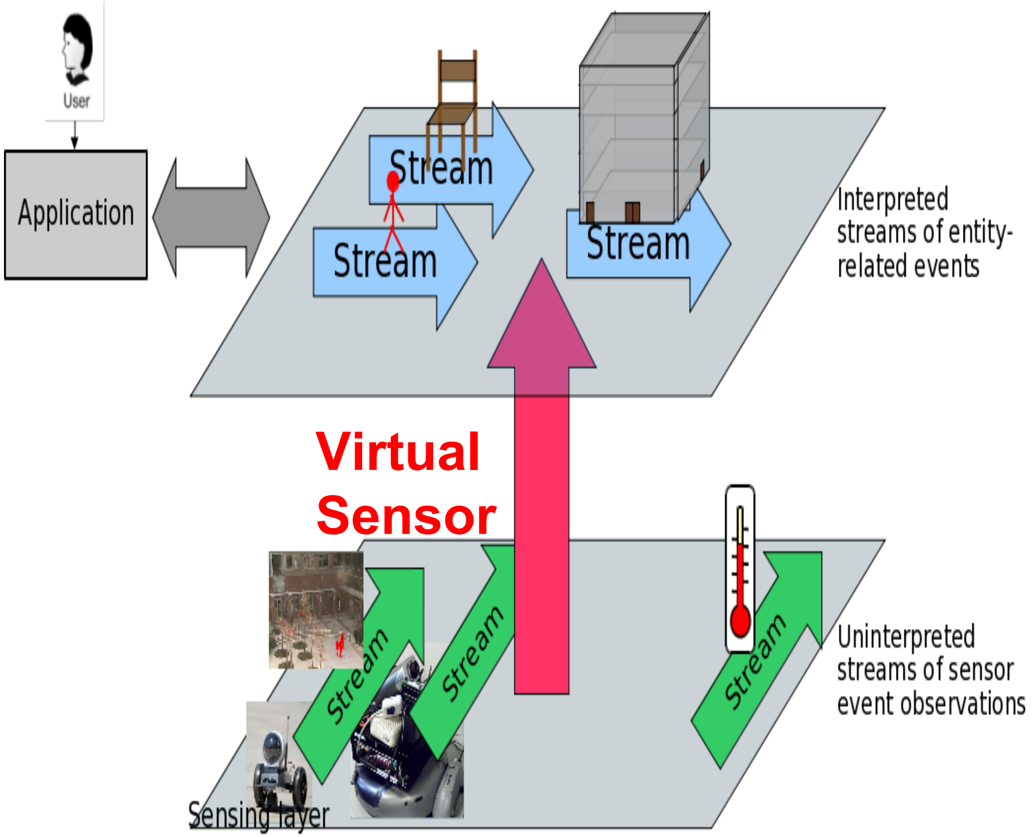
→ Paul is at Alice's office

Solution Approach: Semantic View of IoT Spaces

- **Separation of Concerns**:
  - *Application logic deals largely with the semantic layers.*
  - *System translates semantic concepts into underlying sensor requests.*

- **Hides sensor programming complexity from app. writers**
  - errors, heterogeneity, uncertainty

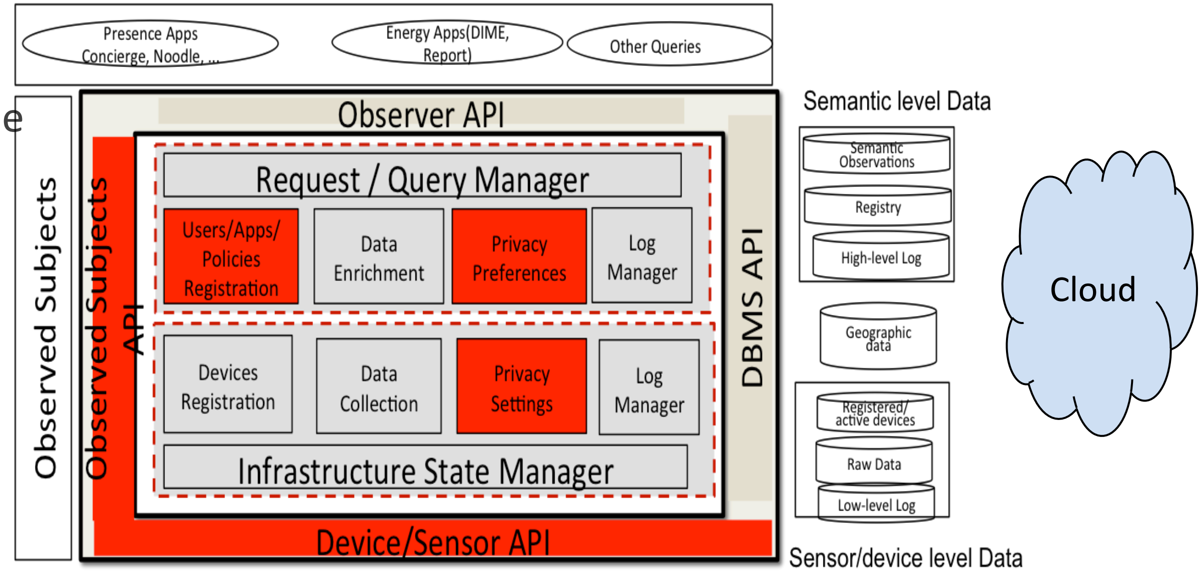
- **Supports extensibility, robustness, adaptation.**


User
Application
Stream
Stream
Stream
Interpreted streams of entity-related events
Virtual Sensor
Stream
Stream
Stream
Uninterpreted streams of sensor event observations
Sensing layer

Provides a natural interface to specify privacy policies and reasoning with such policies.

TIPPERS System Architecture

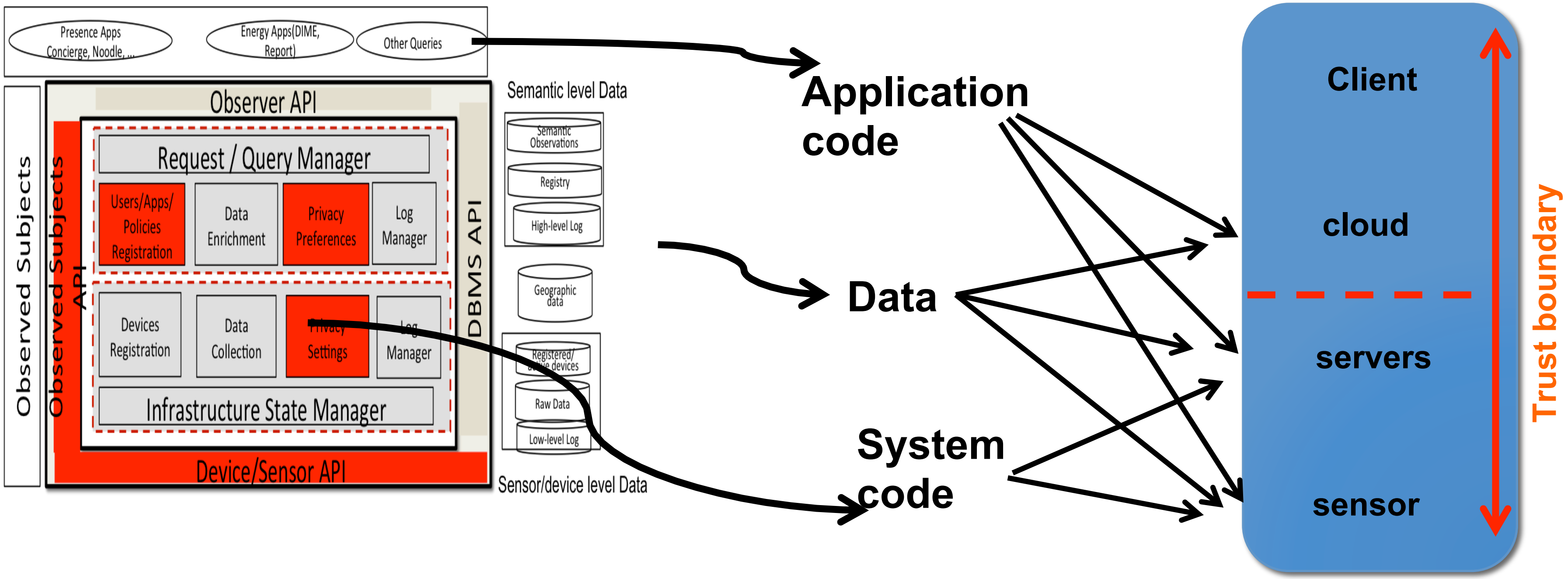
- **Server focused Computing:**
  - Data from sensors migrates to server and stored into a ***database system***
  - Application code & system code runs on the server.



- **NOTE:**
  - **Database system may reside on a third-party site and/or the public cloud**

- **Trust Assumption**
  - Server and sensors are trusted
    - Observed Subjects trust the server to implement user preferences
    - Application users trust the server to implement applications correctly.

Flexible Distributed Computing Architecture



Provides opportunities to explore secure computing under diverse trust assumptions.

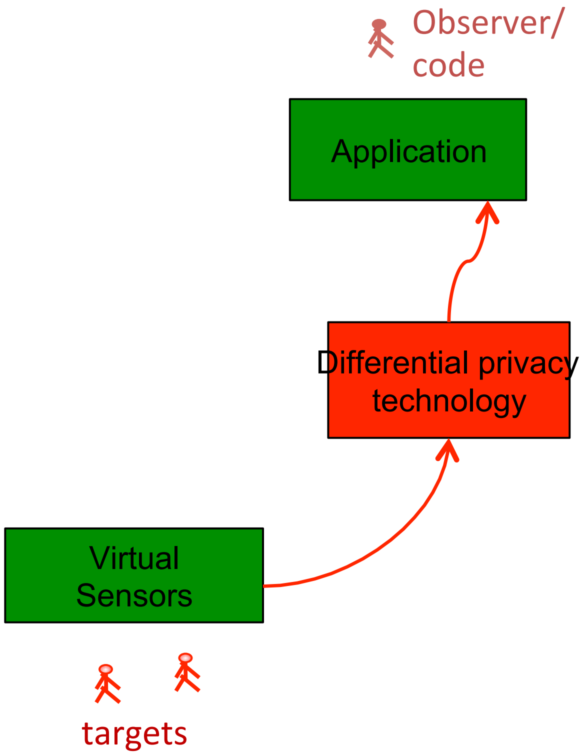
Finer Control to Intercept Communication between Components

Mechanisms to intercept communication between between H/W & S/W components

- seamlessly support privacy technologies

Examples

- Location data intercepted and passed through **DP mechanism** before sharing with occupancy analysis application
- Enforcement of target's privacy policy prior to sharing.



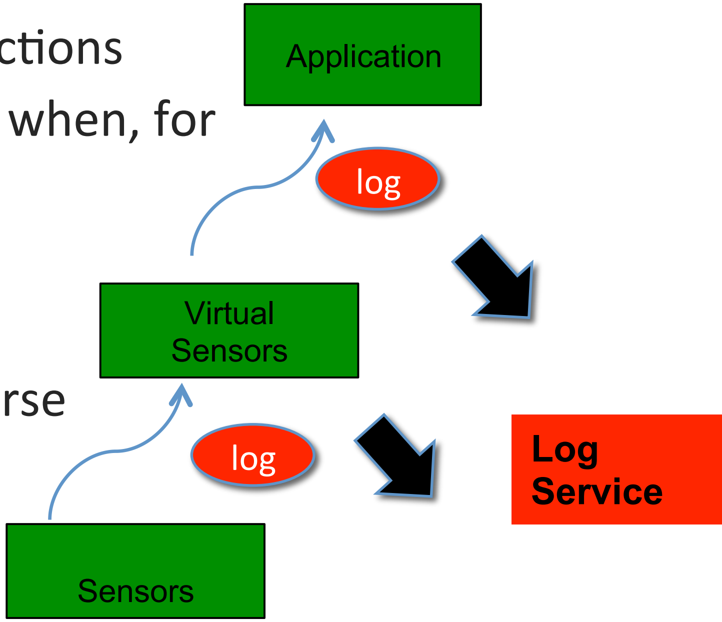
Deep Logging

Mechanisms to intercept and log data flow between components

- Support for provenance in data
- Ability to track what observations led to which actions
- Ability to identify who had access to which data, when, for what purpose.

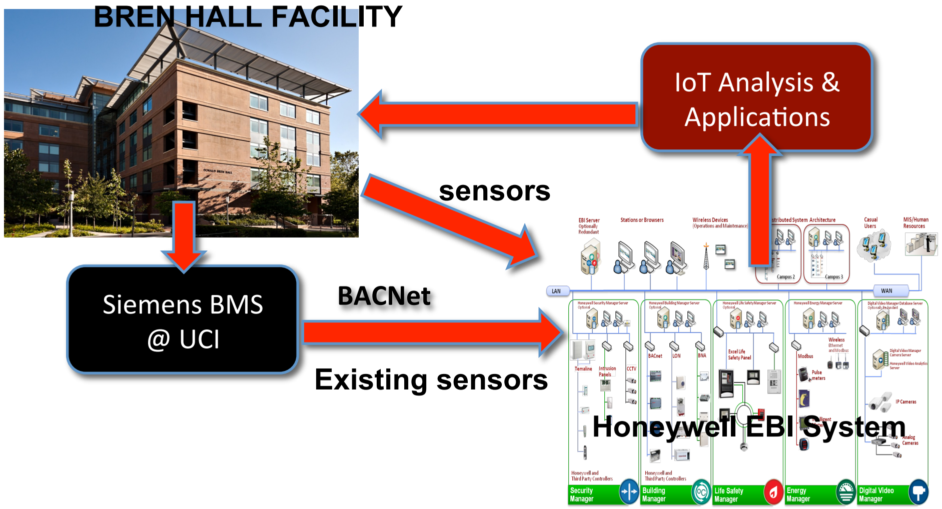
→

- Will enable exploration of how effective are diverse technologies in preventing inferences.



Two Realizations of TIPPERS

Existing System: Honeywell EBI System



BREN HALL FACILITY

Siemens BMS @ UCI

BACNet

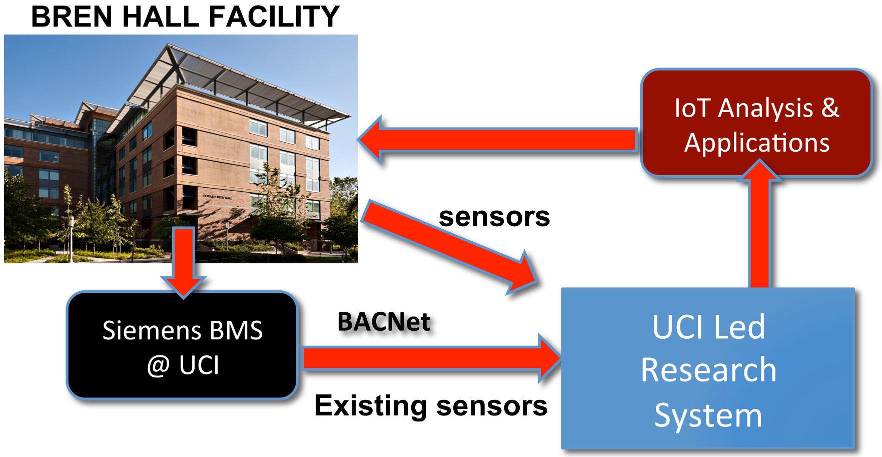
Existing sensors

sensors

IoT Analysis & Applications

Honeywell EBI System

Research System: TIPPERS system



BREN HALL FACILITY

Siemens BMS @ UCI

BACNet

Existing sensors

sensors

IoT Analysis & Applications

UCI Led Research System

Retrofitting Privacy Technologies into EBI

- multiple way to “plug-in” mechanisms
- APIs to call user-scripts within EBI, ODBC access to underlying database
- Mechanism to inject code in sensor data flows
- Mechanism to manage privacy policies

Plug-n-play capability for privacy technologies

- data abstractions at multiple level of semantic abstractions.
- Open architecture for privacy interventions
- Flexibility to deploy app. logic anywhere: sensors, servers, clouds.
- Support for logging of all activities

TIPPERS Sensors

Infrastructure	Mobile Phone	Raspberry-PI (probe request sniffer)	PC
Temperature	GPS	Motion	CPU
Beacon	Accelerometer	Temperature	Memory
HVAC	Light	Gas	Idleness
Pressure	Gyroscope	Humidity	Process
Wi-Fi AP	Proximity	Light	...
Power Outlet	..	...	
Energy meters*			
Camera			

TIPPERS Sensors

Infrastructure	Mobile Phone (participants 5 → 50+)	Raspberry-PI (probe request sniffer) (2→50+)	PC (participants 5 → 50+)
Temperature (216 points) [UCI facilities]	GPS	Motion	CPU
Beacon (16 → ~100)	Accelerometer	Temperature	Memory
HVAC (116-d data readings every 15 min) [UCI Facilities]	Light	Gas	Idleness
Pressure	Gyroscope	Humidity	Process
Wi-Fi AP (64) [UCI OIT]	Proximity	Light	...
Power Outlet (10 – in meeting room)	..	...	
Energy meters* (1 / circuit breaker, approx. 500)			
Camera (40 covering all public areas)			

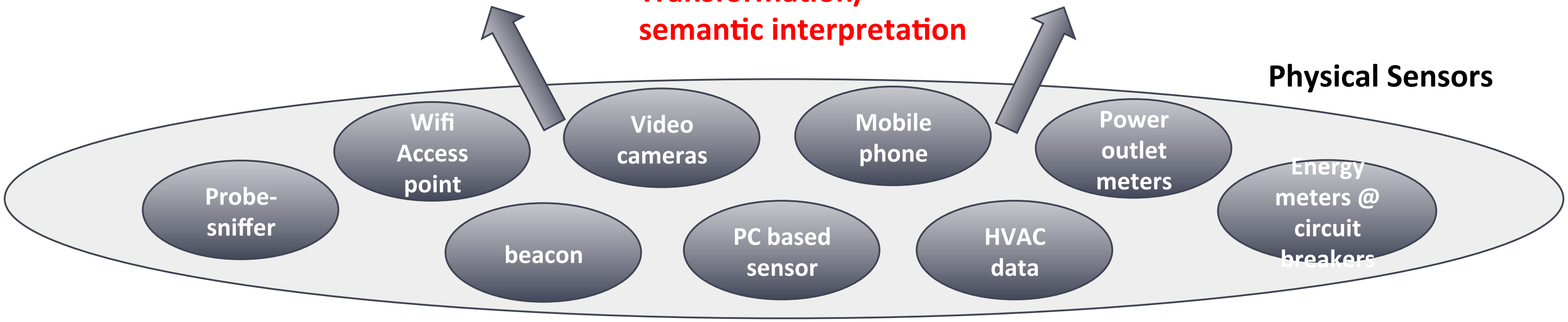
TIPPERS: Two Key Virtual Sensors as Application Enablers

Presence Table

Id	confidence	Location	Person	Activity	timestamp
56abe5 84a4ca a171fc 8c9681	0.85	2099	559efcb 1a11a2b 6faff39d 25	Enter	2016-01-29-14:20:10
56abef 30b4cd c315ae 69819a	0.8	2085	559efcb 1a11a2b 6faff39d 25	Enter	2016-01-29-08:20:10
…	…	…			

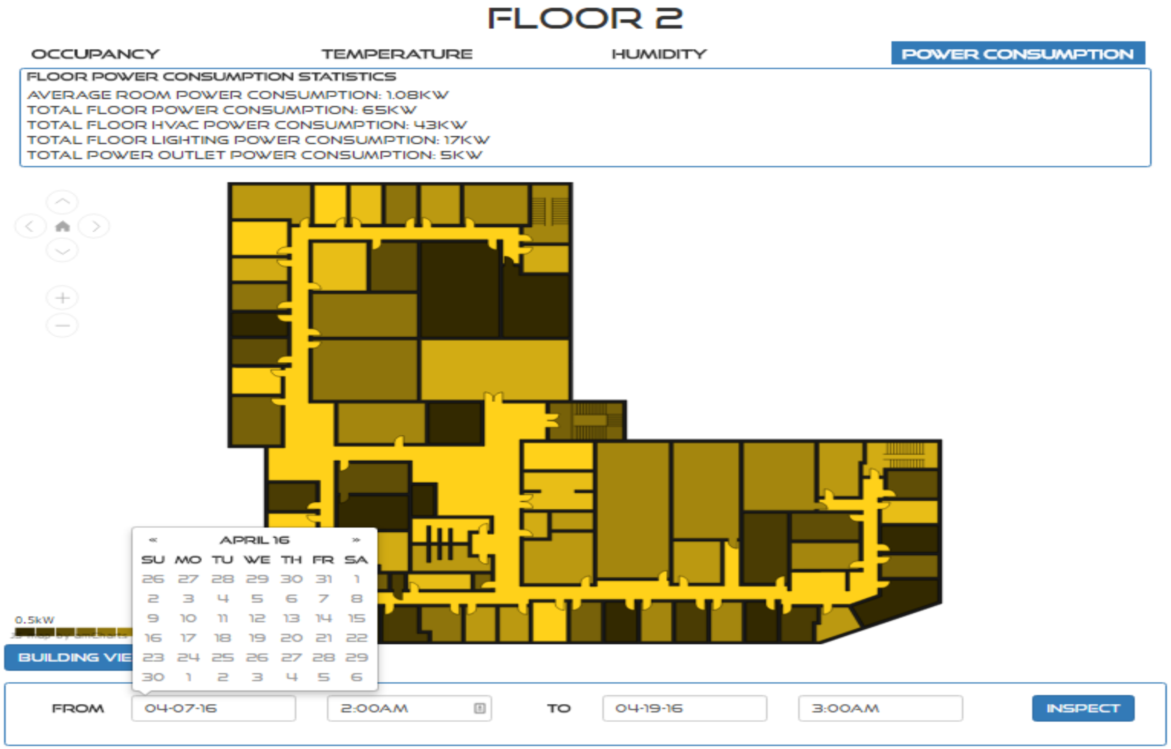
Energy Usage Table

Id	confidence	resource	usage	time
56abe5 84a4ca a171fc 8c9681	0.85	Room 2099	10kw	2016-01-29-14:20:10
56abef 30b4cd c315ae 69819a	0.8	Room 2085	12Ks	2016-01-29-08:20:10
…	…	…		



TIPPERS Application : T-Board

- **T-Board: is a smart dashboard for users and building administrators to monitor energy usage and presence information in the building spaces.**



FLOOR POWER CONSUMPTION STATISTICS

AVERAGE ROOM POWER CONSUMPTION: 1.08KW
TOTAL FLOOR POWER CONSUMPTION: 65KW
TOTAL FLOOR HVAC POWER CONSUMPTION: 43KW
TOTAL FLOOR LIGHTING POWER CONSUMPTION: 17KW
TOTAL POWER OUTLET POWER CONSUMPTION: 5KW

« APRIL 16 »

SU	MO	TU	WE	TH	FR	SA
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

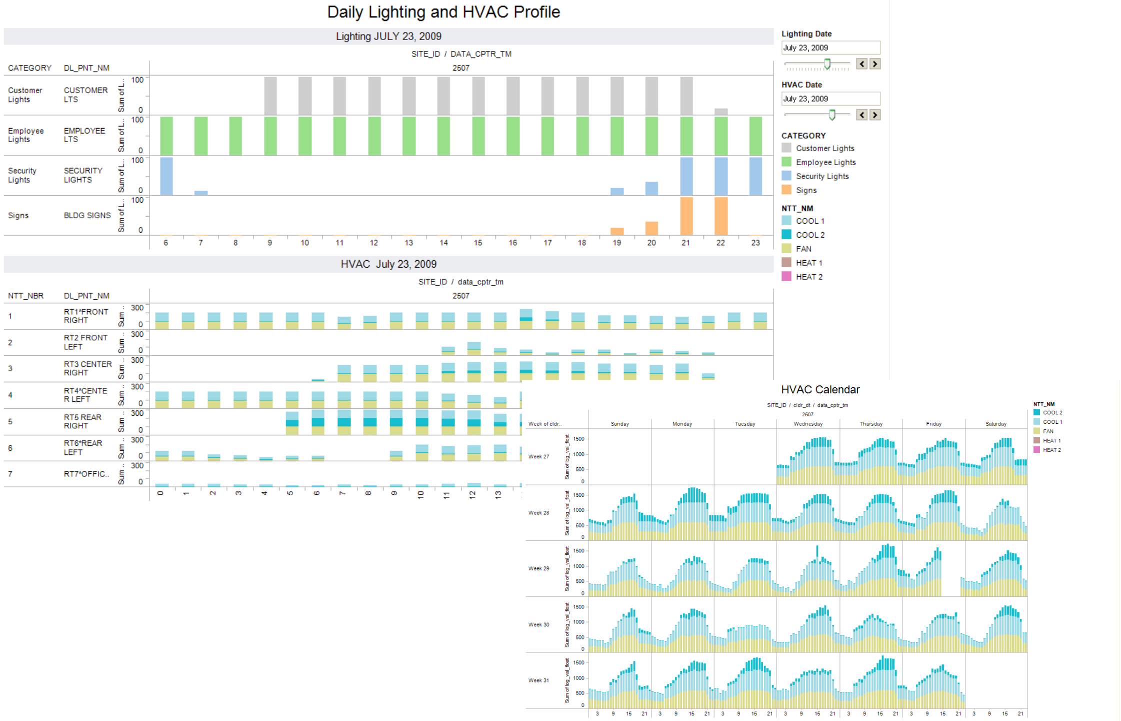
FROM 04-07-16 2:00AM TO 04-19-16 3:00AM

Color coded map of energy usage versus occupancy. Will allow ability to zoom into regions and explore usage over time.

TIPPERS Application : Energy Miner

- Energy Miner: system for co-analyzing energy and occupancy data that supports mechanisms for *outlier detection*, ability to drill down, perform *what-if analysis*

Example Illustration

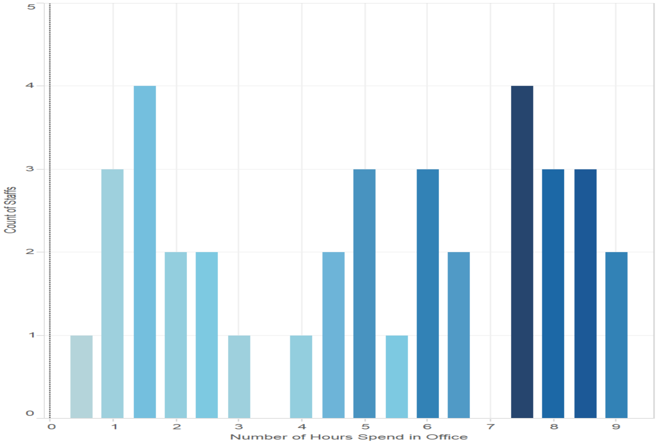


Enables users to see what devices are on and their energy consumption. Will allow users to turn on/off devices to see impact on energy consumption

Sample Privacy Concerns..

Average Time Staff Spends in Office

Number of staff



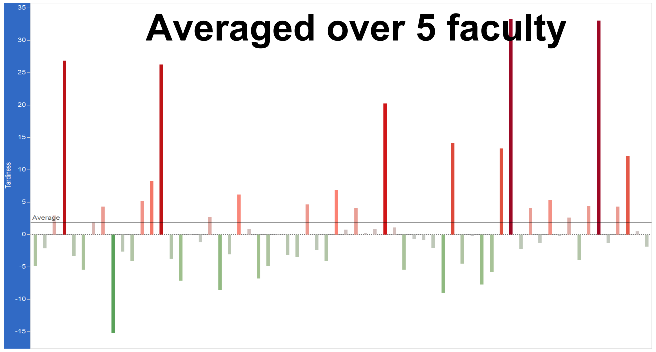
Hours – ½ hour

Average Time Spends in Office by Class

Graduate student > Staff > Faculty > Others

How Tardy are Faculty to their Classes

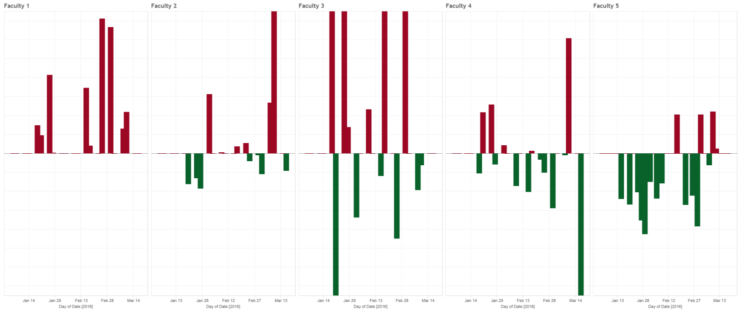
Time in minutes



Classes

This data contains 1 real faculty who gave consent

Time in minutes



Faculty

TIPPERS Cluster

Cluster Participants (core team)

- UCI & Honeywell ***(Testbed & Experimental Systems Creation)***
- CMU ***(Personal Policy Assistant)***
- Massachusetts, Duke, Colgate ***(Differential privacy)***
- Stealth Technology ***(Secure Multiparty Computation)***
- Galois technologies + Cybernetica ***(Metrics & Evaluation)***

Cluster Participants (others)

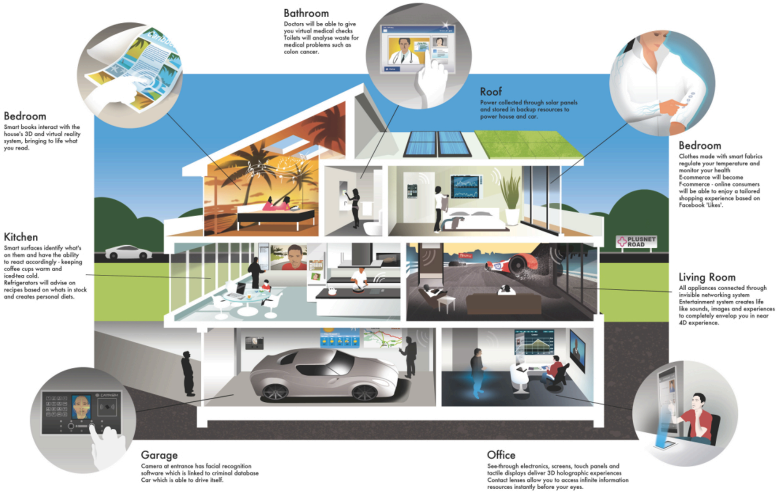
Tippers has attracted attention from additional participants who have expressed keen interest in the infrastructure

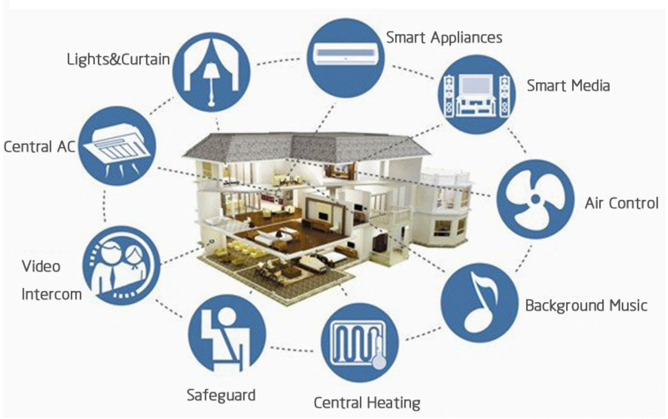
- Toshiba Technologies ***(IoT Data management)***
- Intel ***(IoT sensors, privacy)***
- U. of Albany ***(privacy preserving video Surveillance)***
- UT Dallas ***(secure outsourcing)***
- Univ. of New South Wales ***(security in IoT)***

Summary

- **TIPPERS is an experimental IoT system with plug-n-play approach to support variety of privacy technologies.**
- **Initial System Design focuses on server centric computing, and trusted server infrastructure**
- **Yet, it provides a rich playground for exploring efficacy of diverse privacy technologies**
  - Differential privacy, secure computation, privacy-utility tradeoffs, user policies and preferences
- **Future system enhancements will:**
  - enable exploration of privacy in the context of untrusted environments,
  - privacy technologies for fine grained control over data flow,
  - and deep logging to enable evaluation.
- **Many (unanticipated) new research challenges**
  - Interplay between uncertainty and privacy technology
  - Scalability of privacy policy enforcement
  - ..

Smart Homes - Next Generation


Bathroom
Doctors will be able to give you virtual medical checks Toilets will analyse waste for medical problems such as colon cancer.
Bedroom
Smart books interact with the house's 3D and virtual reality system, bringing to life what you read.
Roof
Power collected through solar panels and stored in backup resources to power house and car.
Bedroom
Clothes made with smart fabrics regulate your temperature and monitor your health E-commerce will become F-commerce - online consumers will be able to enjoy a tailored shopping experience based on Facebook 'Likes'.
Kitchen
Smart surfaces identify what's on them and have the ability to react accordingly - keeping coffee cups warm and iced-tea cold. Refrigerators will advise on recipes based on whats in stock and creates personal diets.
PLUSNET ROAD
Living Room
All appliances connected through invisible networking system Entertainment system creates life like sounds, images and experiences to completely envelop you in near 4D experience.
Garage
Camera at entrance has facial recognition software which is linked to criminal database Car which is able to drive itself.
Office
See-through electronics, screens, touch panels and tactile displays deliver 3D holographic experiences Contact lenses allow you to access infinite information resources instantly before your eyes.



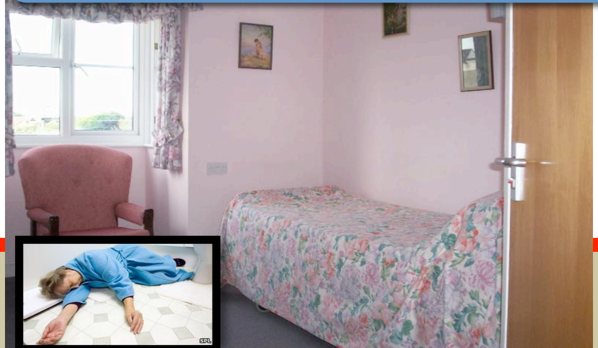
Personalization and Privacy is key

Inhe

Needs differ person-to-person and over time

Privacy expectations – fundamental to home
-- Highly granular sensors data may capture information about individuals, their location, habits, health status, religious affiliation, behavior, likes/dislikes, … ***Things that people often consider private!***

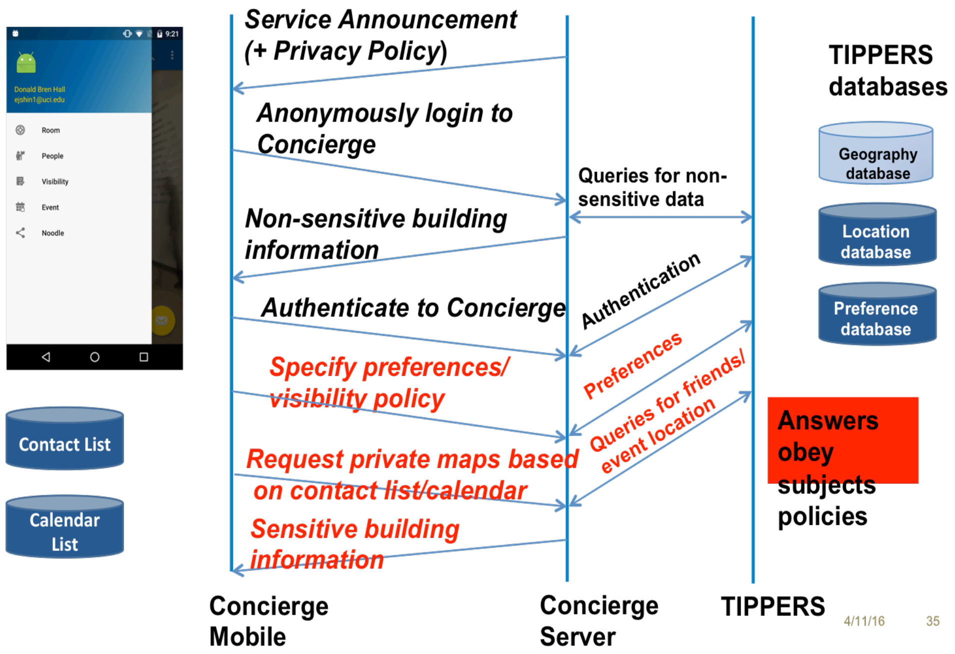
Multisensor Ambient
Fall detection

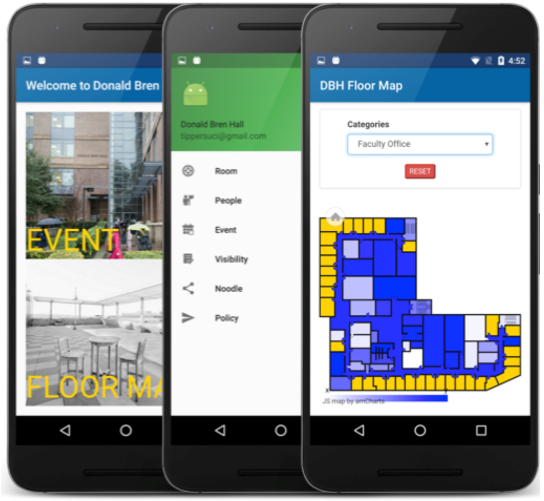


- **Safety/ Resilience,** Comfort / Entertainment, COST, COST, COST

TIPPERS Application : Concierge

- Concierge provides information about building to visitor. (e.g. *restrooms, water faucets, meeting rooms, public events). Additional information about location of individuals in the contact list, events in calendar, etc. available based on policies.*


Donald Bren Hall
ejshin1@uci.edu
Room
People
Visibility
Event
Noodle
Contact List
Calendar List
Service Announcement (+ Privacy Policy)
Anonymously login to Concierge
Queries for non-sensitive data
Non-sensitive building information
Authenticate to Concierge
Authentication
Specify preferences/ visibility policy
Preferences
Queries for friends/ event location
Request private maps based on contact list/calendar
Sensitive building information
TIPPERS databases
Geography database
Location database
Preference database
Answers obey subjects policies
Concierge Mobile
Concierge Server
TIPPERS



Data access based on Policies & user preferences