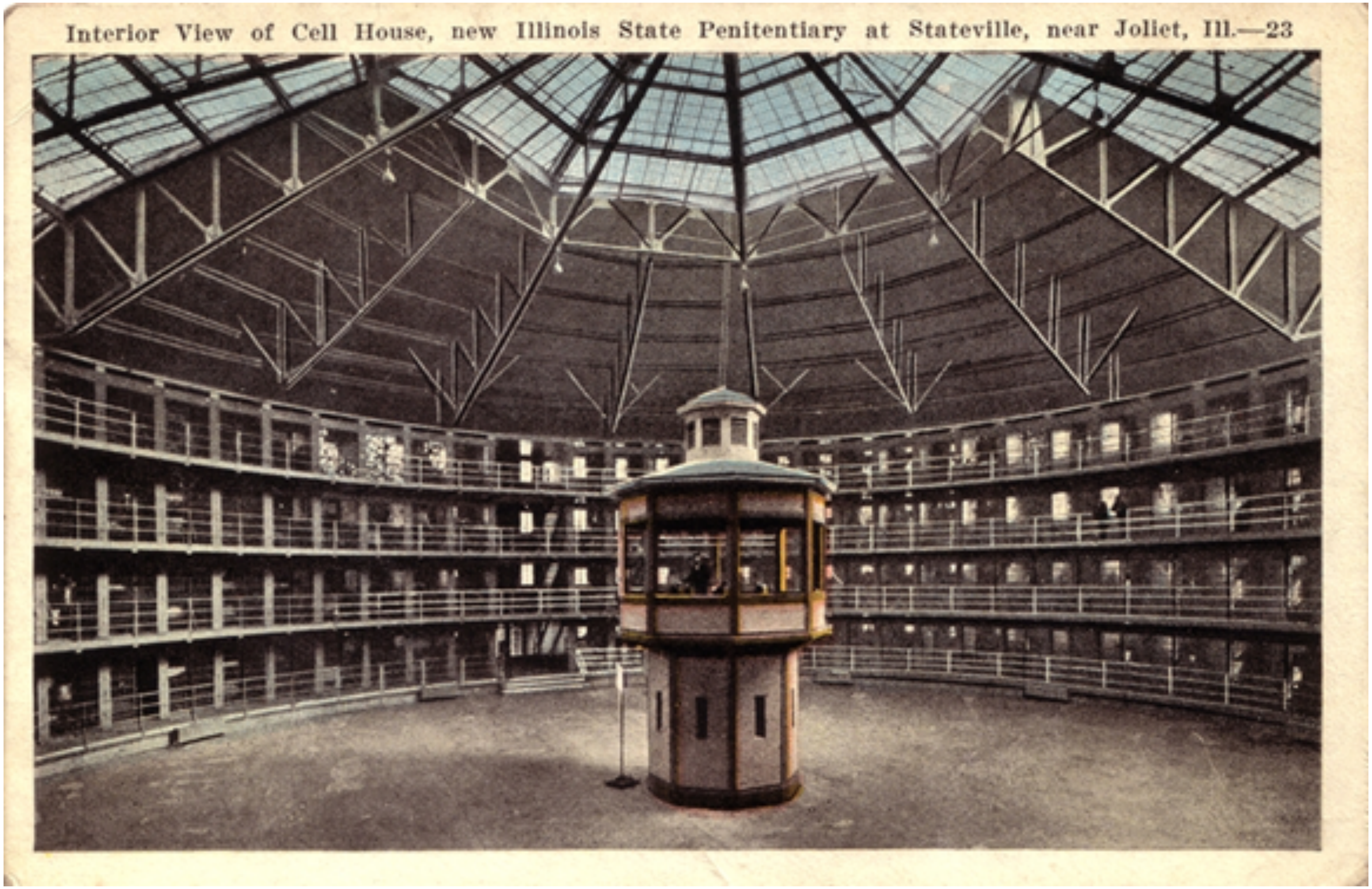


Privacy

EE382V Activity Sensing and Recognition

UT Austin • Dept. Electrical and Computer Engineering • Fall 2016

Today

Any questions?

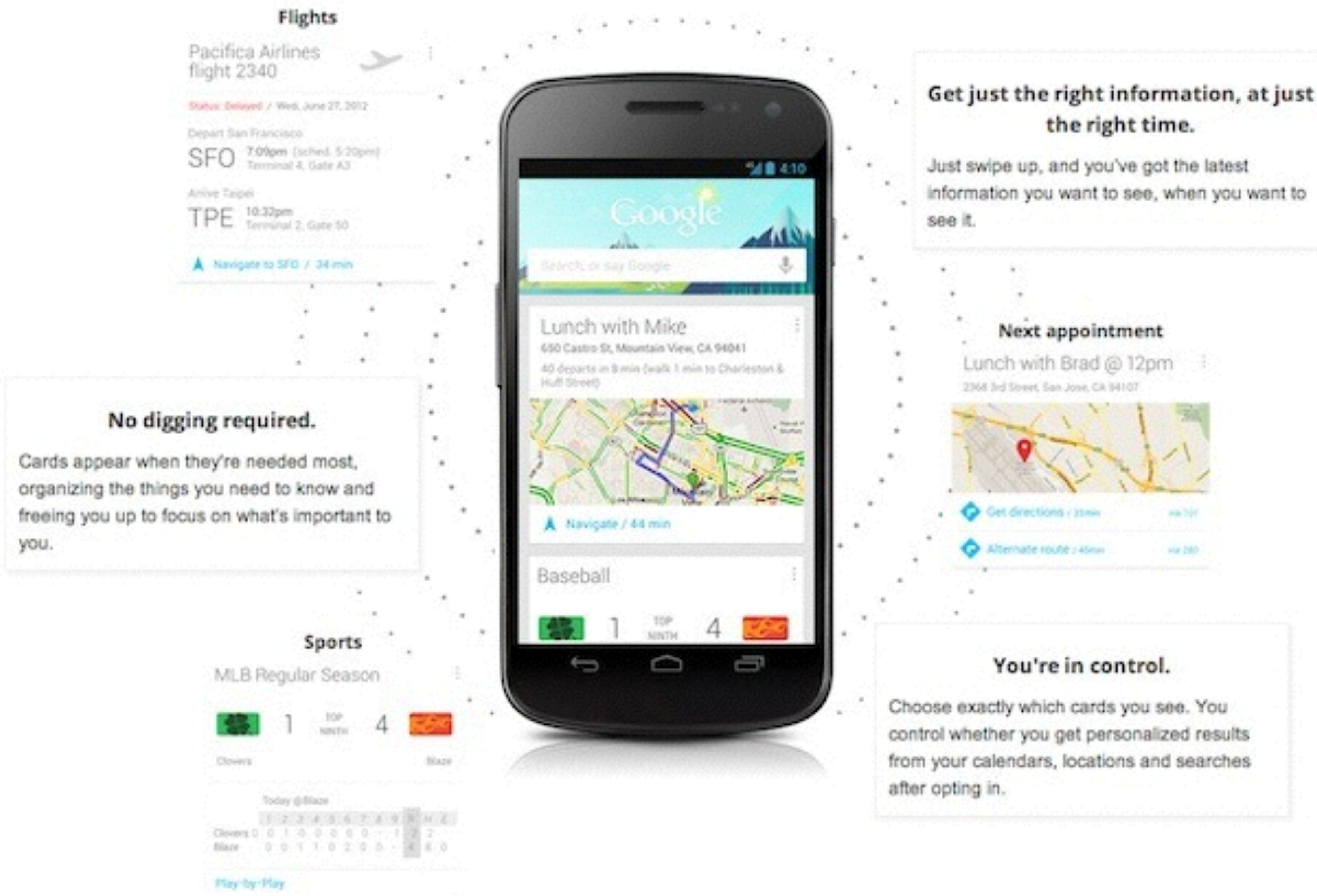
Graded Project Progress Reports

Privacy

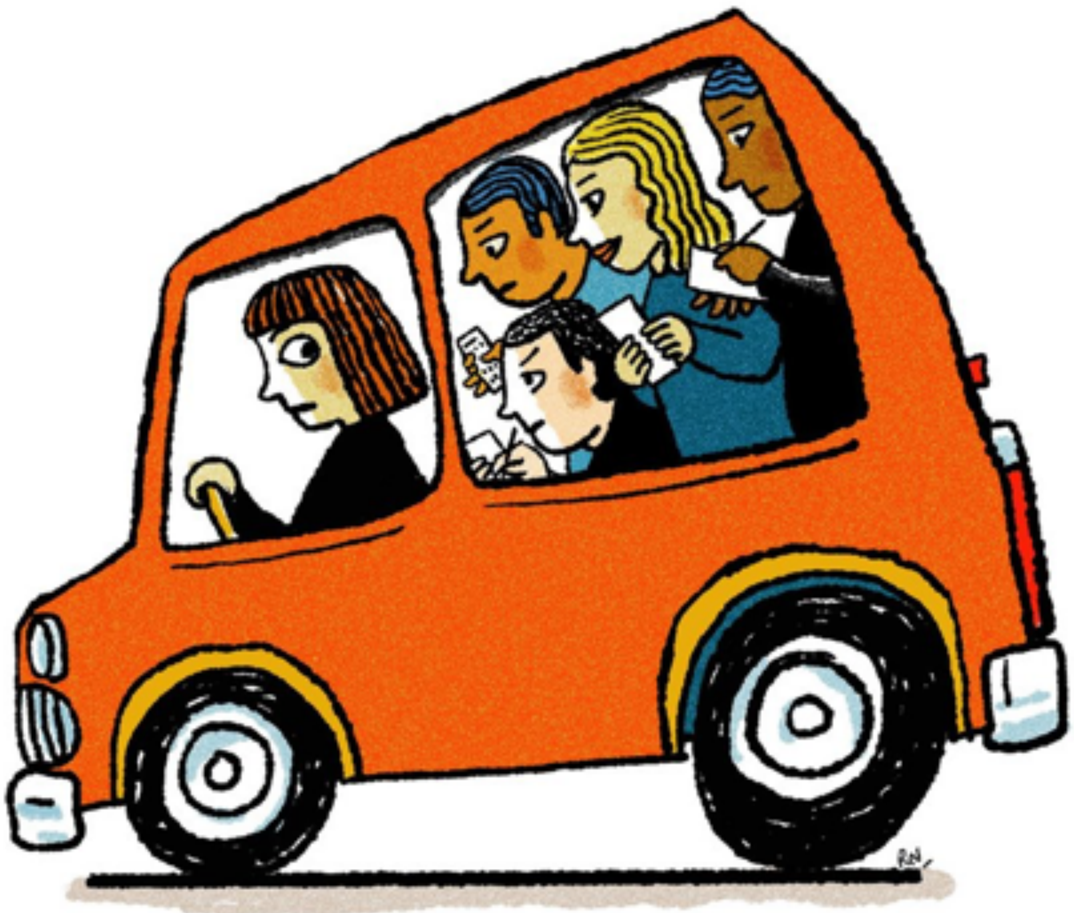
- Discussion about privacy threats in Activity Recognition
- Discussion about 2 privacy papers
- Privacy-Saliency Matrix

Privacy in Activity Recognition

Privacy in Activity Recognition



Privacy in Activity Recognition



Source: New York Times

Privacy in Activity Recognition

Lower Your Car Insurance Bill, at the Price of Some Privacy

GPS Tracker May Help Lower Your Car Insurance

Car Insurers Find Tracking Devices Are a Tough Sell

Progressive and other insurers look for ways to get devices inside vehicles, but customers are wary; 'It just creeps me out'

Progressive Insurance's Driver Tracking Tool Is Ridiculously Insecure

Car Insurance Tracking Devices: Setting Rates According to How You Drive

Privacy in Activity Recognition

Can a Fitness Tracker Save You Money on Health Insurance?

Some employers are offering financial incentives for getting in shape.

Privacy in Activity Recognition

Which modalities or systems that we’ve seen posed privacy concerns?

How could those privacy concerned be mitigated?

Sound Shredding

Sound Shredding: Privacy Preserved Audio Sensing

Sumeet Kumar, Le T. Nguyen, Ming Zeng, Kate Liu, Joy Zhang
Carnegie Mellon University
Moffett Field, California, USA
{sumeet.kumar, le.nguyen, ming.zeng, kate.liu, joy.zhang}@sv.cmu.edu

ABSTRACT

Sound provides valuable information about a mobile user's activity and environment. With the increasing large market penetration of smart phones, recording sound from mobile phones' microphones and processing the sound information either on mobile devices or in the cloud opens a window to a large variety of mobile applications that are context-aware and behavior-aware. On the other hand, sound sensing has the potential risk of compromising users' privacy. Security attacks by malicious software running on smart phones can obtain in-band and out-of-band sound information to infer the content of users' conversation. In this paper, we propose two simple yet highly effective methods called *sound shredding* and *sound subsampling*. Sound shredding mutates the raw sound frames randomly just like paper shredding and sound subsampling randomly drops sound frames without storing them. The resulting mutated sound recording makes it difficult to recover the text content of the original sound recording, yet we show that some acoustic features are preserved which retains the accuracy of context recognition.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; H.5.5 [**Information interfaces and presentation (e.g., HCI)**]: Sound and Music Computing

Keywords

Sound sensing; sound shredding; sound subsampling; user privacy; context recognition

1. INTRODUCTION

Mobile sound sensing, which uses acoustic attributes collected by mobile devices has been found useful in diverse scenarios of context awareness. Because audio data may contain unique fingerprints, allowing sound sensing software to extract and recognize meaningful events, many applications and systems have already applied sound sensing to improve their approaches. For instance, SurroundSense [2] uses acoustic and other attributes to identify user motions and SenseOrchestra [4] leverage sounds and images to recognize the location from where those data were collected. These research results clearly demonstrate that sound sensing could be of significant value in context recognition.

In a typical audio-based application, sounds are collected by mobile devices (either phones or tablets), and stored in storage like SD cards. These mobile devices are usually equipped with high sample rate microphones, which are useful for audio-based applications such as phone conversation, speech recognition, and sound sensing etc. However, the benefit entails the risk of privacy when it comes to collecting audio data. The raw audio data from the microphone are insecure and could easily be replayed. The replayed sound, even at a low sampling rate, may reveal the identity and other sensitive information about the users. Thus the raw sounds may be abused to disrupt the privacy guarantees for users. The problem becomes more obvious in case of continuous sampling applications such as MobiSens [13].

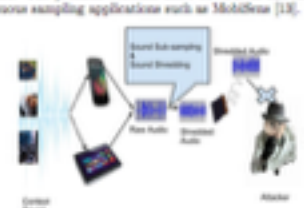


Figure 1: Shredded and sub-sampled audio could not be easily reconstructed, making it difficult for an attacker to sniff any sensitive information.

The main contributions of this paper are:

- **Two methods to preserve audio privacy:** We address the concern of privacy guarantees that may be undermined by malicious software intending to sniff information from raw sounds, by preprocessing raw sounds with sound shredding and subsampling.
- **Experiments and evaluation of proposed methods:** The goal of the two proposed methods is to preserve the user's privacy without significantly decreasing context recognition accuracy. Therefore, we

HotMobile'15, February 12–13, 2015, Santa Fe, New Mexico, USA.

http://dx.doi.org/10.1145/2699343.2699366.

Encountering SenseCam

Encountering SenseCam: Personal Recording Technologies in Everyday Life

David H. Nguyen[1], Gabriela Marcu[1], Gillian R. Hayes[1], Khai N. Truong[2], James Scott[3], Marc Langheinrich[4], Christof Roduner[4]

[1]Dept. Informatics, UC Irvine, {dhn, gmarcu, gillianrh}@ics.uci.edu

[2]Dept. Computer Science, University of Toronto, khai@cs.toronto.edu

[3]Microsoft Research Cambridge, jws@microsoft.com

[4]Institute for Pervasive Computing, ETH Zurich, langheinrich@acm.org, roduner@inf.ethz.ch

ABSTRACT

In this paper, we present a study of responses to the idea of being recorded by a ubicomp recording technology called SenseCam. This study focused on real-life situations in two North American and two European locations. We present the findings of this study and their implications, specifically how those who might be recorded perceive and react to SenseCam. We describe what system parameters, social processes, and policies are required to meet the needs of both the primary users and these secondary stakeholders and how being situated within a particular locale can influence responses. Our results indicate that people would tolerate potential incursions from SenseCam for particular purposes. Furthermore, they would typically prefer to be informed about and to consent to recording as well as to grant permission before any data is shared. These preferences, however, are unlikely to instigate a request for deletion or other action on their part. These results inform future design of recording technologies like SenseCam and provide a broader understanding of how ubicomp technologies might be taken up across different cultural and political regions.

Author Keywords

Paratyping, SenseCam, Experience Sampling, Privacy

ACM Classification Keywords

K.4.2 [Computers and Society]: Social Issues; K.8.m [Personal Computing]: Miscellaneous

General Terms

Human Factors

BACKGROUND AND INTRODUCTION

In the past decade, there has been a rapid proliferation of small, digital, ubiquitous recording technologies, including everything from camera-phones to sensor networks. At the

Figure 1. (left) The SenseCam form factor used in this study; (right) Sample SenseCam image.

same time, researchers have been examining how novel recording technologies can be used to support a variety of human needs. One such technology, SenseCam, is a wearable digital camera that automatically captures photographs through a wide-angle lens (see Figure 1) [13]. These pictures can be taken on a schedule or in response to sensed stimulus (*e.g.*, movement, sound, light).

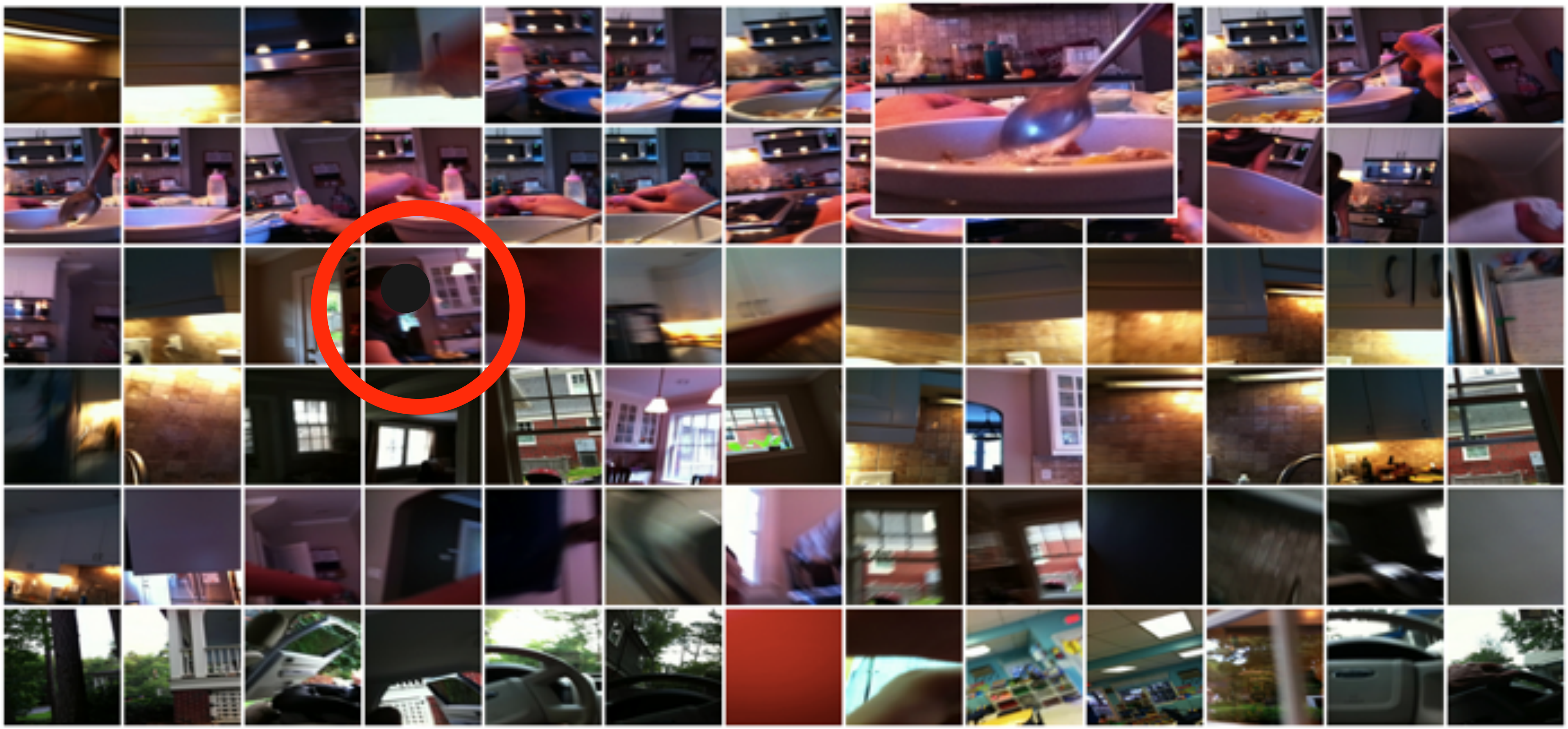
The original goal of the SenseCam project was to augment human memory through passive recording of images. Experiments were undertaken to ensure that the sensors would trigger the capture of an image at appropriate intervals (*e.g.*, when transitioning between rooms in a house) [11] and to uncover basic design requirements for the wearer of SenseCam [13]. The current design is approximately the size of a deck of playing cards with battery life and storage capacity of a day. To address concerns about privacy and control of data, SenseCam developers explicitly excluded recording audio. Additionally, a simple button allows pausing of the recording of images.

SenseCam research generally has been focused on the needs of the primary user of SenseCam and its potential applications. Researchers have conducted numerous studies of SenseCam for use with patients with memory impairment (*e.g.*, [13, 20]), in educational settings [3], in business negotiations with blind users [22], and more. During previous studies of SenseCam, however, an interesting phenomenon was observed repeatedly: most of the people with whom the wearer interacted either did not notice the device or noticed it but comprehended neither its capabilities nor uses. Therefore, the extensive work in designing and evaluating SenseCam

UbiComp 2009, Sep 30 – Oct 3, 2009, Orlando, Florida, USA.

Privacy-Saliency Matrix


BUS



Privacy Issues

Technological Approaches for Addressing Privacy Concerns When Recognizing Eating Behaviors With Wearable Cameras

Addressing Privacy Issues (in Practice)

Apply image processing techniques

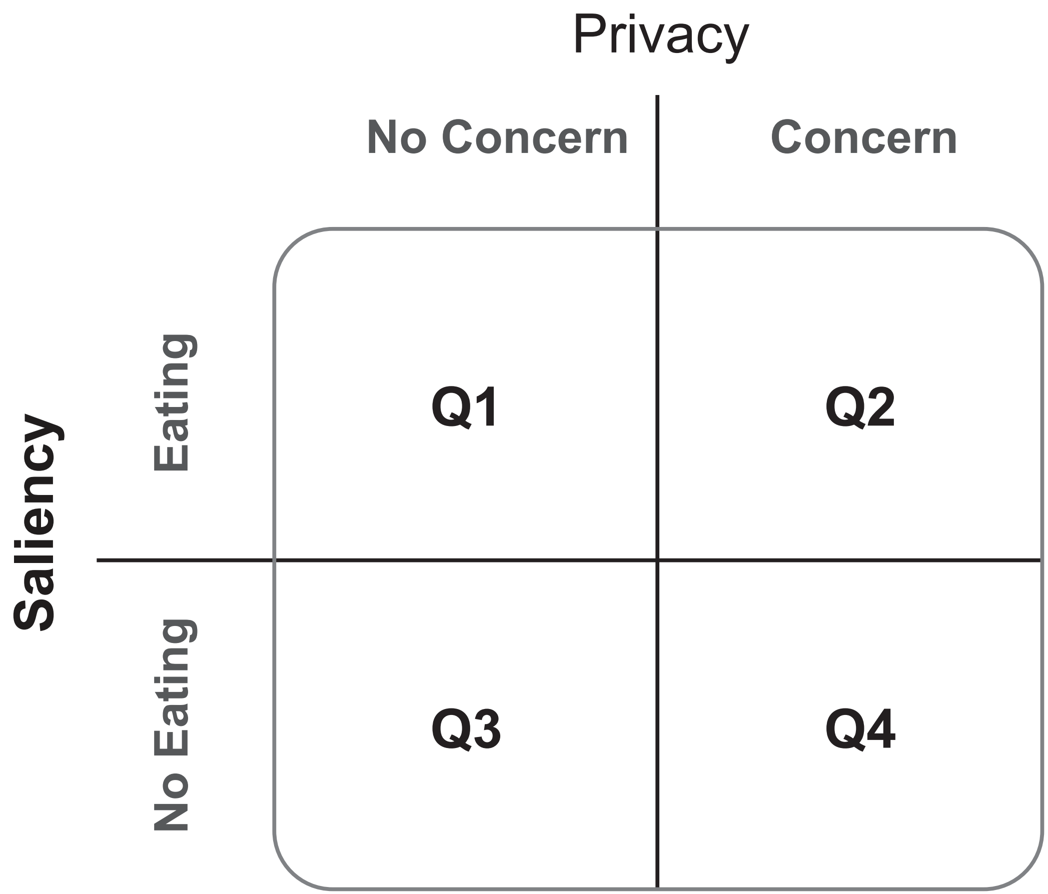
e.g. Face Detection, Selective Blurring

Image processing not perfect

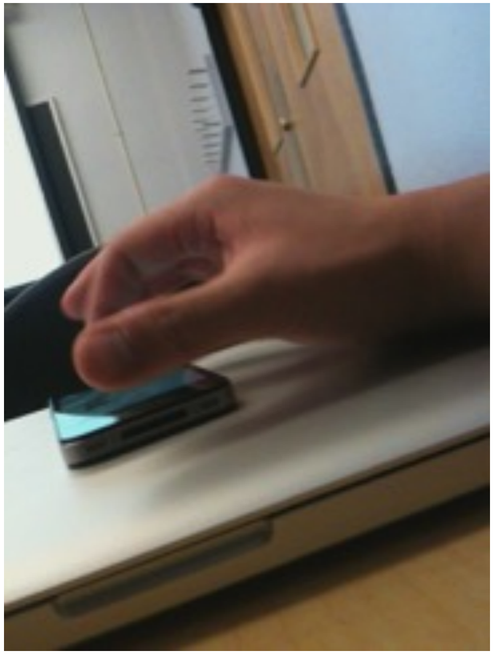
False positives, false negatives, etc...

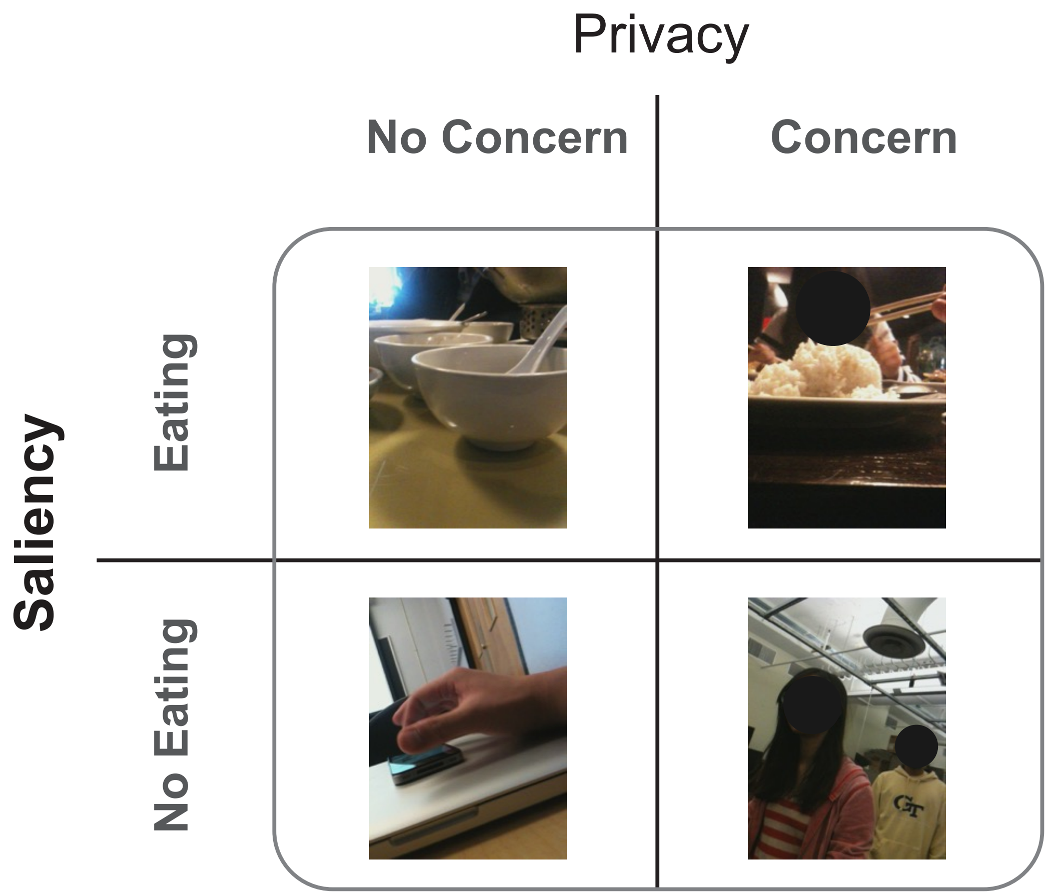
How to quantify, understand balance between privacy vs. saliency in images?

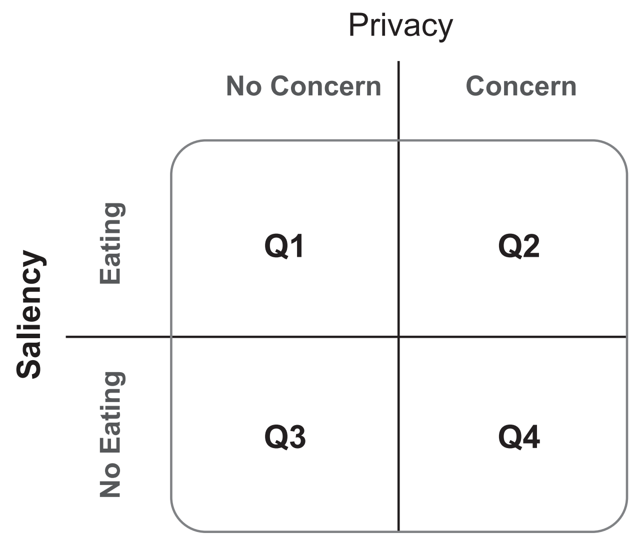
Privacy-Saliency Matrix

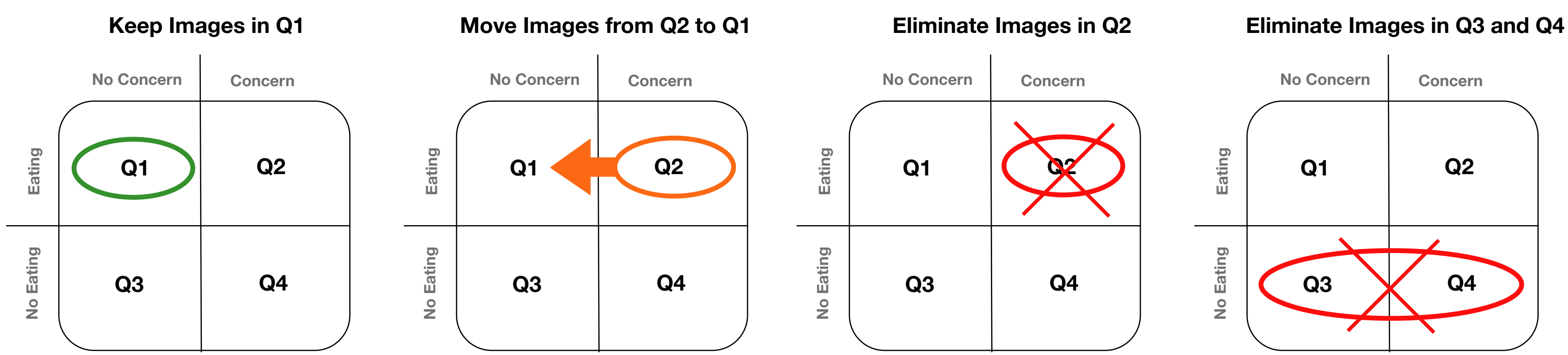


Privacy
No Concern
Concern
Saliency
Eating
No Eating
Q1
Q2
Q3
Q4




Privacy
No Concern
Concern
Saliency
Eating
No Eating


Privacy
No Concern
Concern
Saliency
Eating
No Eating
Q1
Q2
Q3
Q4


Keep Images in Q1
Move Images from Q2 to Q1
Eliminate Images in Q2
Eliminate Images in Q3 and Q4
No Concern
Concern
Eating
No Eating
Q1
Q2
Q3
Q4

User Study

Participants

Participant	Age	Gender	# of Images
P1	31	Male	1230
P2	24	Male	5360
P3	21	Male	2528
P4	23	Male	1958
P5	25	Male	3346

Image + Sensor Capture

iPhone 3GS, held with lanyard

Custom application

Geo-tagged photo every 30 seconds

Saved accelerometer data continuously

Image Coding

14,422 images over 3 days/avg

Ground Truth

0.73 (Fleiss' kappa) inter-rater agreement for 3 coders

Criteria for privacy was strict (Any body part visible)

Ground Truth

	No Concern	Concern
Eating	282	174
No Eating	11495	2471

Four Image Processing Techniques

Face Detection
Haar's cascade classifiers (OpenCV)

Image Cropping
Crop top-half of the image

Location Filtering
Filter based on distance from known eating location

Motion Filtering
Filter based on level of motion calculated from accelerometer data

Face Detection

Haar's cascade classifiers

Viola and Jones' booster cascade approach

Ground Truth

	No Concern	Concern
Eating	282	174
No Eating	11495	2471

Face Detection

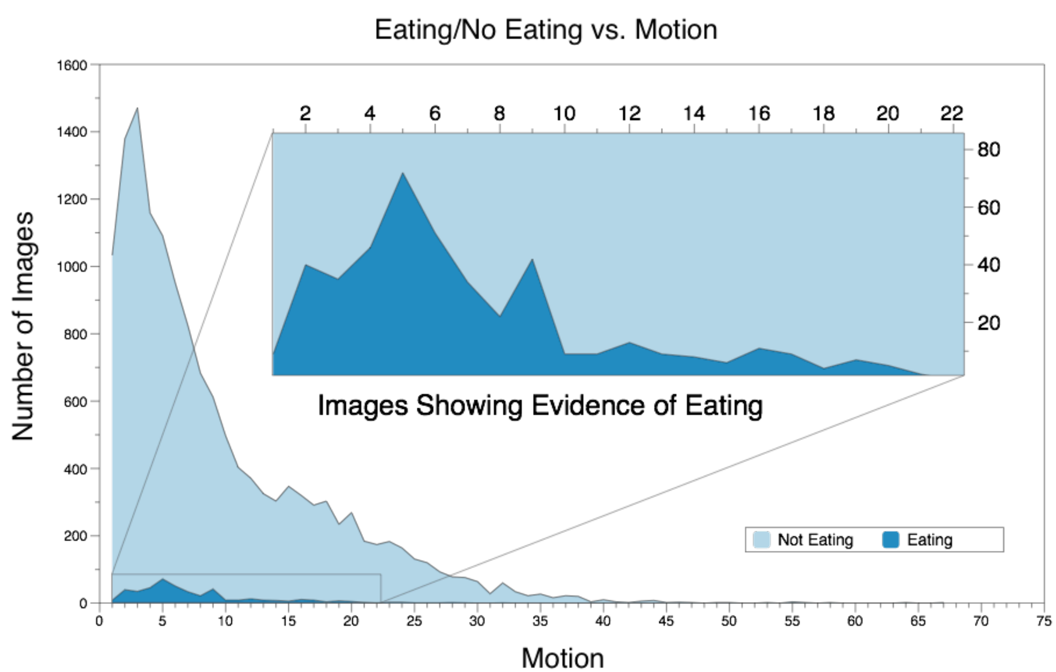
	No Concern	Concern
Eating	245 (-13.12%)	102 (-41.37%)
No Eating	9876 (-14.08%)	1607 (-34.96%)

Motion Filtering

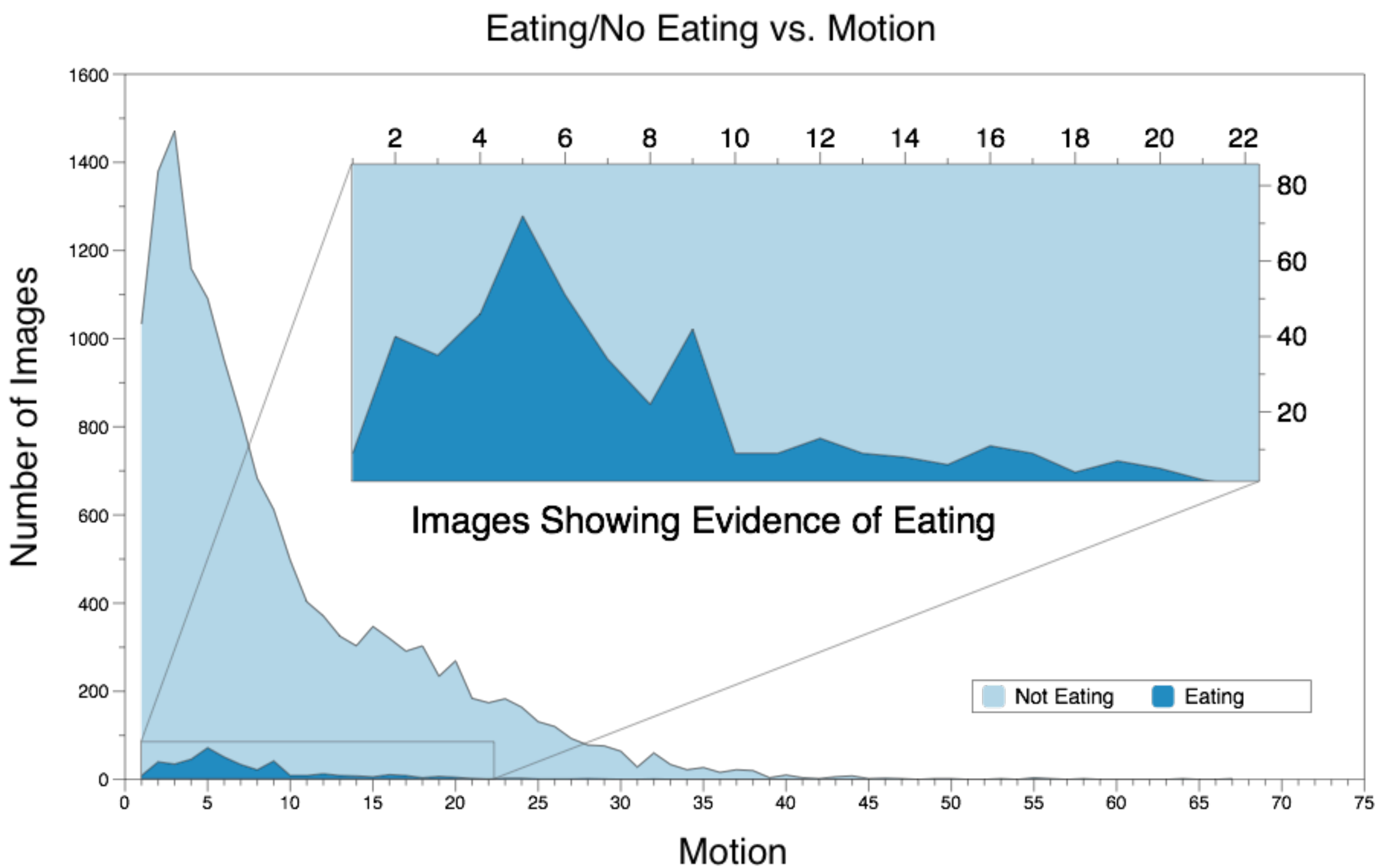
Intuition

Eating less likely when lots of physical movement are observed

Computed motion measure based on accelerometer data for each image



Motion Filtering



Motion Filtering

Ground Truth

	No Concern	Concern
Eating	282	174
No Eating	11495	2471

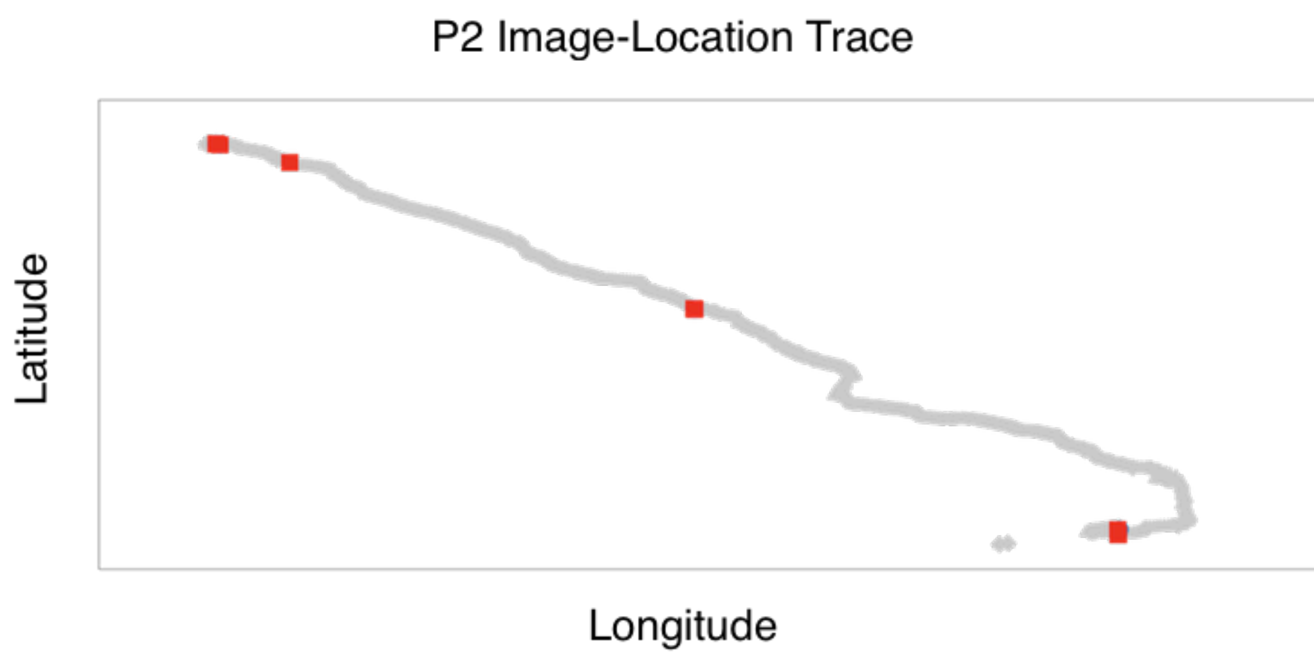
Motion Filtering

	No Concern	Concern
Eating	213 (-24.47%)	138 (-20.69%)
No Eating	7407 (-35.57%)	1446 (-41.49%)

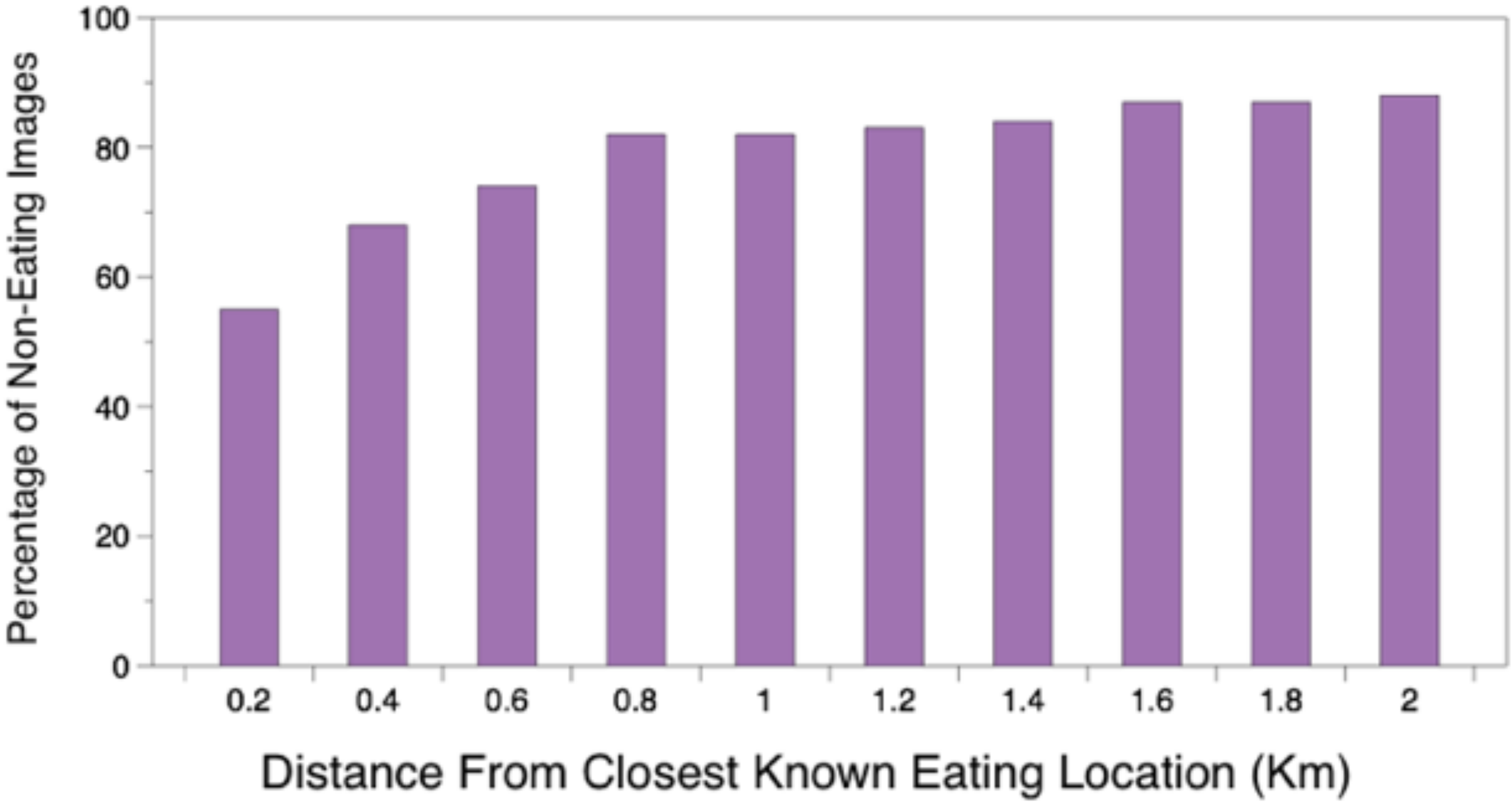
Location Filtering

Intuition

Eating tends to happen in a small set of known locations. These locations can be inferred (e.g. restaurant, Placer algorithm by Krumm & Rouhana - Ubicomp2013)



Location Filtering



Location Filtering

Ground Truth

	No Concern	Concern
Eating	282	174
No Eating	11495	2471

Location Filtering

(based on data from 4 participants)

	No Concern	Concern
Eating	216 (0%)	171 (0%)
No Eating	5795 (-46%)	1227 (-40.89%)

Cropping Filtering

Intuitions

We can eliminate privacy-sensitive regions of images (instead of discarding images altogether)

Assumption

The bottom half of FPPOV images is where the food is

Keep bottom half of images

Cropping Filtering

Ground Truth

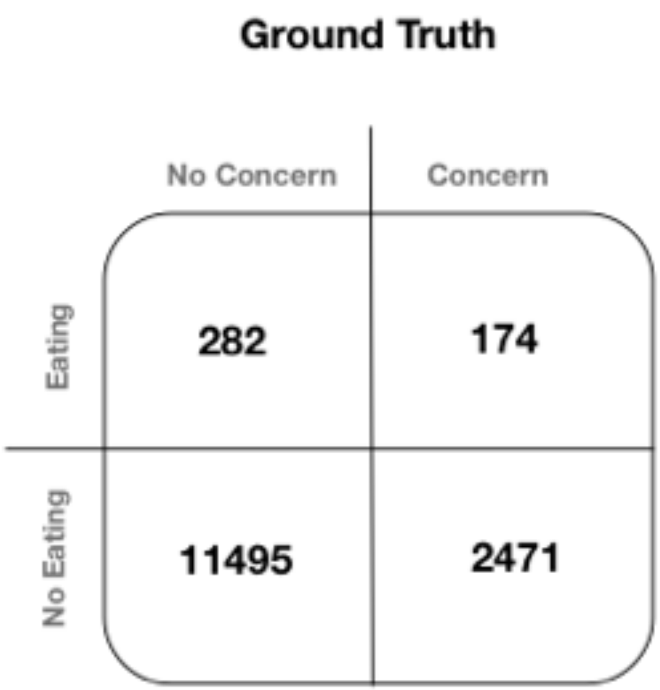
	No Concern	Concern
Eating	282	174
No Eating	11495	2471

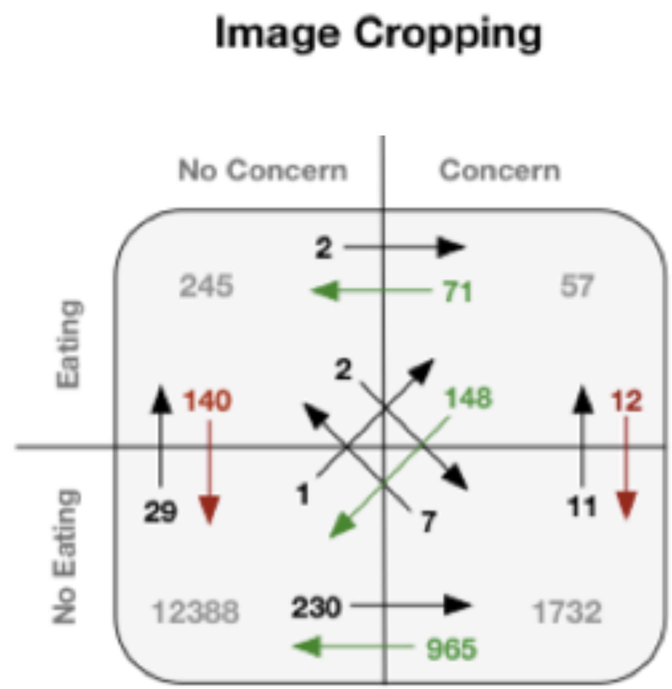
Image Cropping

	No Concern	Concern
Eating	245 (-13.12%)	57 (-64.24%)
No Eating	12388 (+7.76%)	1732 (-29.9%)

Cropping Filtering :: Transitions

Cropping Filtering :: Transitions





Important Points

Additional privacy risks

e.g. computer screen, credit card, cell phone usage

Impact of Camera position

Head camera sample images

Neck camera sample images

Head Camera

	No Concern	Concern
Eating	90	64
No Eating	1982	769

Neck Camera

	No Concern	Concern
Eating	197	2
No Eating	4894	49

Next class

Emerging Topics

Questions and Review for Final Exam