

Mobile Crowdsensing

Ethical Issues in Mobile Sensing

CSE 162 – Mobile Computing

Hua Huang

Department of Computer Science and Engineering

University of California, Merced

Mobile Crowdsensing

Recap: mobile personal sensing

- **Personal sensing:** phenomena for an individual. Focusing on user's daily life, physical activity
 - E.g: Logging for health monitoring
 - Hand movement tracking
 - Activity recognition (smoking)
 - Localization

Introduction to Mobile Crowdsensing

- Mobile Crowdsensing means the integration of sensors that can be used for gathering materialistic or non-materialistic information, people who use these sensors & obviously their global participation.

Introduction to Mobile Crowdsensing...

Mobile Crowdsensing means the integration of sensors that can be used for gathering materialistic or non-materialistic information, people who use these sensors & obviously their global participation.

User at Front End



Where



Introduction to Mobile Crowdsensing...

Mobile Crowdsensing means the integration of sensors that can be used for gathering materialistic or non-materialistic information, people who use these sensors & obviously their global participation.

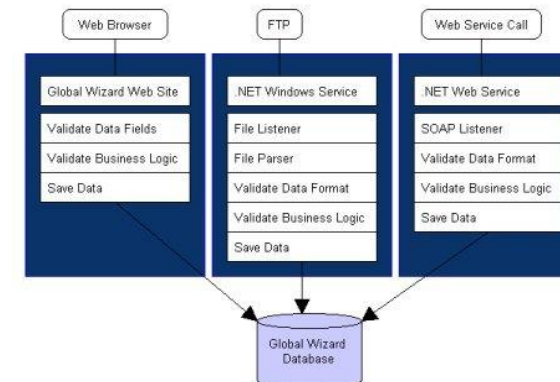
Where



User at Front End



Web Service at Back End



Participatory Sensing

Users actively engage in the data collection activity.

Users manually determine how, when, what, where to sample.

Can avoid phone context issues.

Higher burdens or costs.

Opportunistic Sensing

Takes random sample which is application defined.

Easy to gather large amount data in small time.

Can't avoid phone context issues.

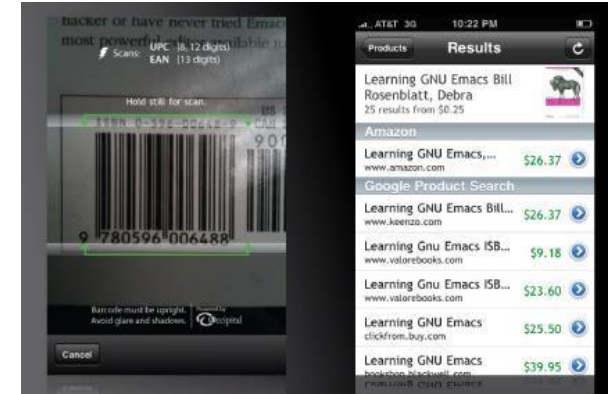
Lower burdens or costs if contextual problems are handled.

Filtering Data by Handling Privacy Issues & Localization.

Dataset is ready for research !!!

Participatory crowdsensing examples

- **LiveCompare**
 - User-created database of UPCs and prices
 - GPS and cell tower info used to find nearby stores
- **PetrolWatch**
 - Uses phone to photograph gasoline price
 - Uses GPS to know when gas station is near



Opportunistic crowdsensing examples



- **Pothole Monitor**

- Combines GPS and accelerometer

- **Party Thermometer**

- Asks you questions about parties
- Detects parties through GPS and microphone

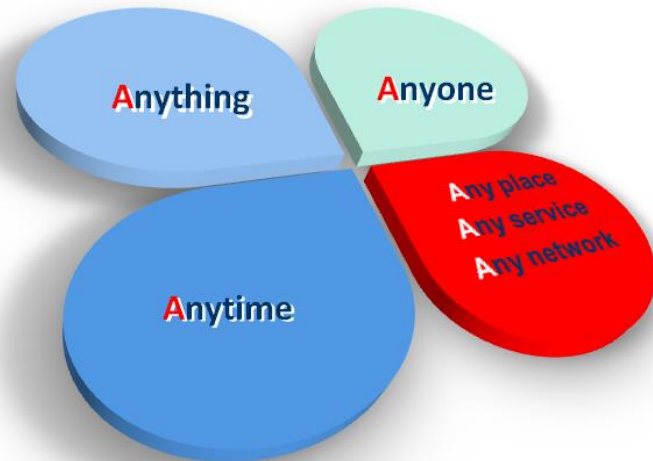
The Concept of “Internet of Things”...



“When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What’s revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention.”

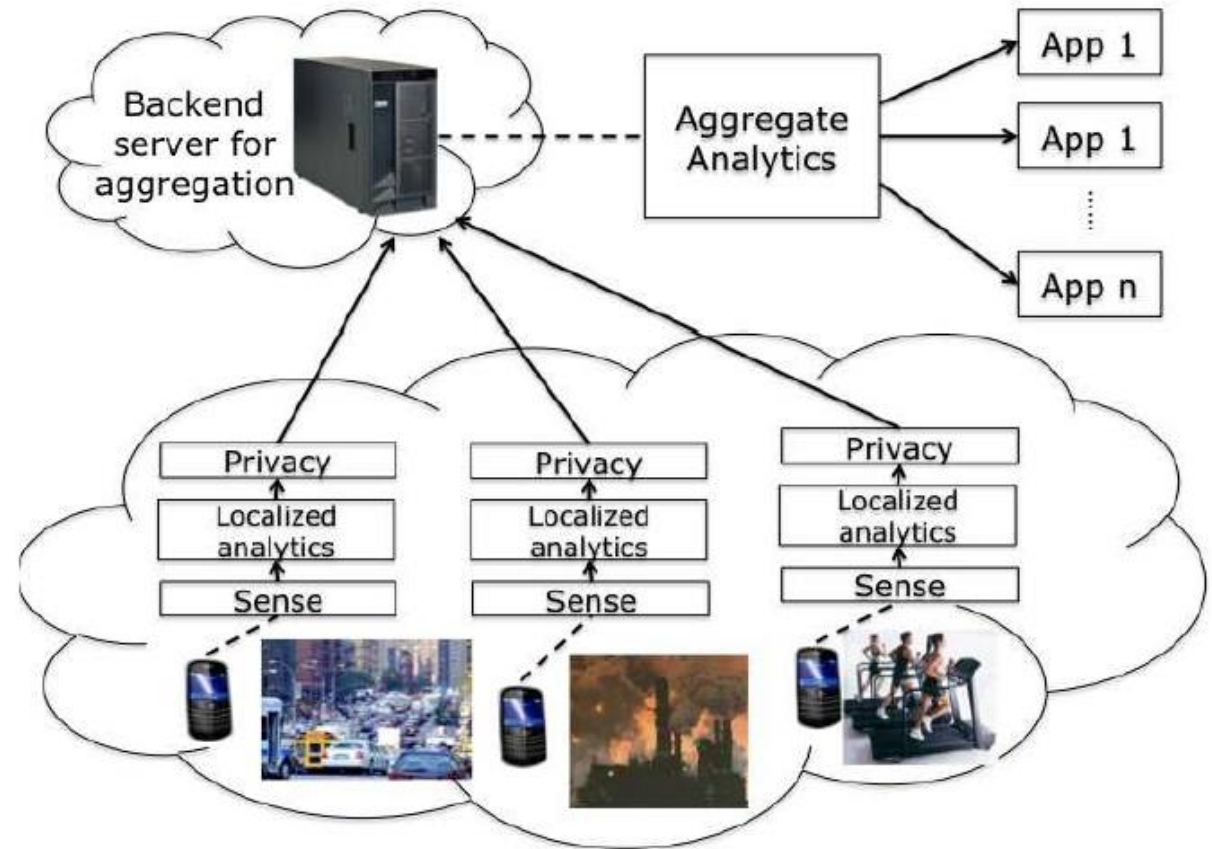
--- (McKinsey & Company,

Connecting:



MCS Architecture

- Raw sensing data is collected on devices.
- Local analytics process it to produce consumable data for applications.
- After privacy preservation, the data is sent to the backend.
- Aggregate analytics will further process it for different applications.



The Challenges of MCS...

Incentivize Users

Resource Limitations

Privacy

Aggregate Analytics

Challenge: Incentivize users

- Entertainment as an incentive
 - Pokeman Go
 - focus on enriching game players' experience by incorporating various devices with sensing capabilities.
- Service as incentive
 - Traffic monitoring
 - A participant is both a contributor and a consumer.
- Monetary incentive
 - measure web content usage by paying users money based on page visits to a site.
 - Auction-based method often used

Challenge: Resource limitations

- How do multiple applications on the same device utilize energy, bandwidth, and computation resources without significantly affecting the data quality of each other?
- How does scheduling of sensing tasks occur across multiple devices with diverse sensing capabilities and availabilities (which can change dynamically)?

Privacy Preserving Approaches

- Anonymization ; which removes any identifying information from the sensor data before sharing it with a third party.
- Secure multiparty computation, where cryptographic techniques are used to transform the data to preserve the privacy of an individual.
 - Example: privacy leakage from text auto-completion
 - Example: suggested location of interest

This is a double sided sword.....

Pro

- Help people collect higher quality or semantically complex data
 - Otherwise expensive and time consuming surveys are needed

Con

- User's privacy and preferences can conflict with MCS.
 - Need to live within these constraints.

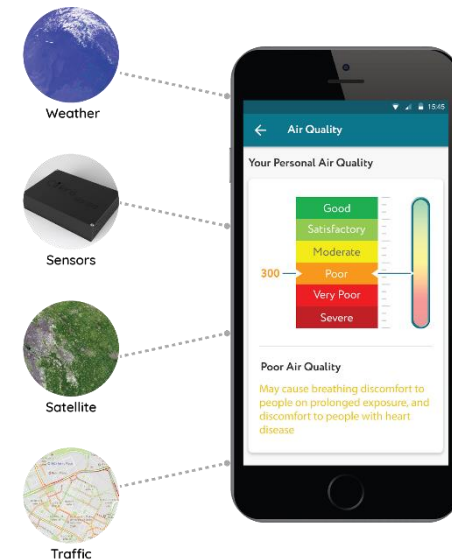
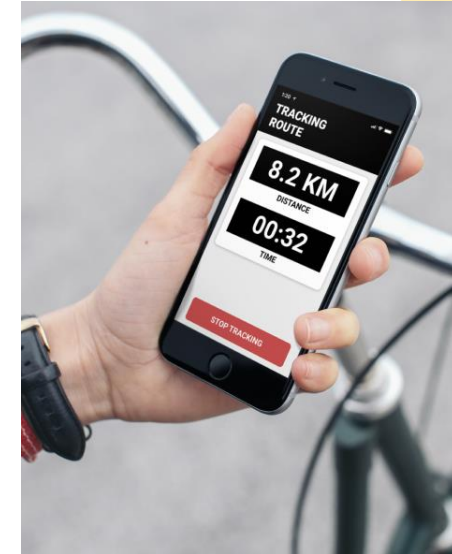
Ethical Issues in Mobile Sensing

What sensitive information can be collected by mobile systems?

- Video
 - Sounds
 - GPS
 - Locations
 - Physiology
 - User's self reported information
 - Many more!
-
- All with one unified API, and cheap

Mobile sensing for social projects

- Assess pedestrian or bike friendliness of neighborhoods.
- Use the location awareness to understand the user's exposure to air pollution as they move around.
- Use phones to snap, tag and upload photos of community events



Ethical Issues in Mobile Sensing

- Privacy: control over personal data
- Consent: Informed permission
- Equity: fairness in how individuals are treated
- Social forgetting: purposeful discarding of information about individuals in order to enable forgiveness, recovery, or a clean slate.

Privacy

- Mobile systems can gather significant amounts of data about the users.
- However, the data can be subpoenaed, or be demanded by U.S. authorities without warrant
- Unauthorized sharing or data theft can occur at a variety of places
- Complicated end-user licensing agreements may lead users to give away broad rights to share their data in return for services.

Privacy Enhancing Technologies (PETs)

- Approaches to protect the data
- Examples:
 - **Communication anonymizers** hiding the real online identity (email address, IP address, etc.) and replacing it with a non-traceable identity
 - **Shared bogus online accounts.** One person creates an account, and share user-IDs and passwords with everyone.
 - **Obfuscation:** Adding distracting or misleading data to a log or profile.
 - **Access to personal data:** The service provider's allows users to inspect, correct or delete all their data stored at the service provider.

Considerations: Privacy vs Functionality

- Commerce can suffer from strong privacy rights, as there is less information for both producers and consumers in the marketplace
 - Example waze app requires users' location data to function?
- Truthfulness, openness, and accountability can suffer at the hands of strict privacy protections
 - Example: new algorithms for mobile sensing that allow users to replace sensitive location data with believable but fake data

Consent

- Consent is a value central to research ethics in the United States. A critical component of respect, beneficence and justice is informed consent.

Challenges in Consent

- Consent in mobile sensing is complicated by relying on ubiquitous devices.
 - Opting out of the mobile phone network is not a realistic option.
 - In 2011, Apple and Android were storing location data over and beyond what users were notified of and consented to
- Financial interest can conflict with consents
 - Use data to produce targeted advertising, sell valuable behavioral data to third parties, or use location to hone price or product discrimination
- Secondary, unforeseen purposes of data use
 - motion data can infer Parkinson's disease

Soft Surveillance

- A technique used by agents of power, such as governments, to collect seemingly voluntary but actually compelled data.
 - Example: searches to enter planes
 - Example: Withheld Social Security benefits if people do not “voluntarily” submit personal information
- Mobile sensing systems can easily become soft surveillance systems
 - Everywhere, all time presence
 - People can be involved by simply agreeing to data collection

Equity

- Fairness and justice in how individuals are treated
- If powerful institutions gather data from relatively less powerful individuals, mobile sensing could tilt towards control and increased surveillance
- Alternatively, distributed sensing and analysis could shape technologies of care or even empowerment.
- Besides, the availability of mobile phones enables systematic data collection with radically lower cost, which enables data-driven decision-making to small institutions and community groups

Social Forgetting

- Purposeful discarding of information to enable forgiveness and a clean slate
- Mobile sensing can create a record of people's movements, habits, and routines that persists
 - A subject of both celebration and concern

Pros and Cons of persistent records

- Pros
 - Augment human memory. Can improve healthcare, and enable memory bank to relive past events.
- Cons
 - Unintended loss of fresh start
 - Increased surveillance

Solution

- The “right to be forgotten”.
 - A combination of policies and technologies that allow for the gradual decay of digital data.

More info

- EU General Data Protection Regulation
- California Consumer Privacy Act

Privacy Policy

Creating a Privacy Policy

- A privacy policy is a document created to go with a product (app, website, etc.) that describes how the product and company behind it will do the following with a customer or client's data:
 - Gather
 - Use
 - Disclose
 - Manage

Creating a Privacy Policy

- Ask yourself some questions:
 - What data is collected?
 - How it is collected?
 - What you will/can do with it?
 - What will happen to it after X amount of time?
 - Is it anonymous?
 - Are there ads?
 - Is the data shared with another organization?
 - ... and more...

You need a privacy policy because...

- You are collecting personal data
- You are using a third-party service
- Government regulations
- App Store regulations
- Risk alienating customers
- Open to lawsuits

What's in a policy?

- **Information** - what personal information is being collected on the site
- **Choice** - what options the customer has about how/whether her data is collected and used
- **Access** - how a customer can see what data has been collected and change/correct it if necessary

What's in a policy?

- **Security** - state how any data that is collected is stored/protected
- **Redress** - what customer can do if privacy policy is not met
- **Updates** - how policy changes will be communicated

Example Policies

- Google: <https://www.google.com/policies/privacy/>
- Apple: <http://www.apple.com/legal/privacy/en-ww/>
- Facebook: <https://www.facebook.com/policy.php>
- Twitter: <https://twitter.com/privacy?lang=en>

Example Policies

- Note that these are mainly in “regular, plain English!”
- Movement away from “legalese”
- Some privacy policies were automatically processed

What does a privacy policy get you?

- Disclosure of what's going on
- A level of trust with developer
- Meeting requirements from publishers / government agencies

Example

- Google Analytics is one of the most popular digital analytics software.
 - Allows you to analyze details about the visitors on your website and design strategy to improve business
- If you've enabled any Google Analytics Advertising features, you are required to notify your users:
 - What features you've implemented.
 - How you and third-party vendors use first-party
 - How visitors can opt-out of the Google Analytics Advertising

Beyond Policies

- Writing down what you do is good...
- ... following it is even better
- Remember: privacy is not security
- The privacy policy says what you are collecting and what you plan to do
- And absence of this does not mean you shouldn't protect data you collect!

Homework