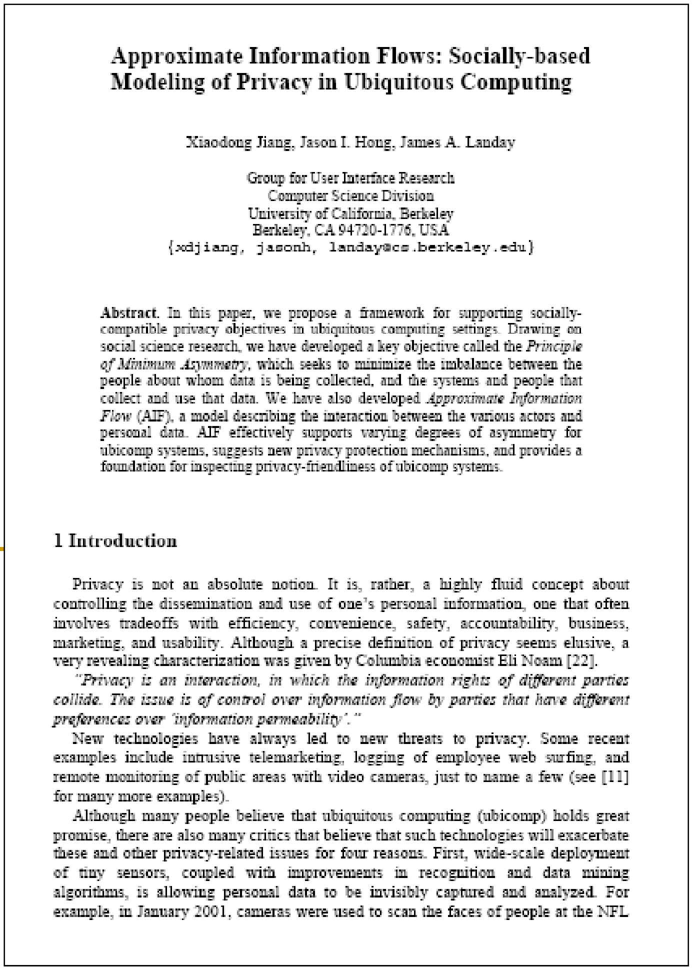
Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing

Xiaodong Jiang, Jason I. Hong, James A. Landay



Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing

Xiaodong Jiang, Jason I. Hong, James A. Landay

Group for User Interface Research
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720-1776, USA
{xdjiang, jasonh, landay@cs.berkeley.edu}

Abstract. In this paper, we propose a framework for supporting socially-compatible privacy objectives in ubiquitous computing settings. Drawing on social science research, we have developed a key objective called the *Principle of Minimum Asymmetry*, which seeks to minimize the imbalance between the people about whom data is being collected, and the systems and people that collect and use that data. We have also developed *Approximate Information Flow* (AIF), a model describing the interaction between the various actors and personal data. AIF effectively supports varying degrees of asymmetry for ubicomp systems, suggests new privacy protection mechanisms, and provides a foundation for inspecting privacy-friendliness of ubicomp systems.

1 Introduction

Privacy is not an absolute notion. It is, rather, a highly fluid concept about controlling the dissemination and use of one's personal information, one that often involves tradeoffs with efficiency, convenience, safety, accountability, business, marketing, and usability. Although a precise definition of privacy seems elusive, a very revealing characterization was given by Columbia economist Eli Noam [22].

"Privacy is an interaction, in which the information rights of different parties collide. The issue is of control over information flow by parties that have different preferences over 'information permeability'."

New technologies have always led to new threats to privacy. Some recent examples include intrusive telemarketing, logging of employee web surfing, and remote monitoring of public areas with video cameras, just to name a few (see [11] for many more examples).

Although many people believe that ubiquitous computing (ubicomp) holds great promise, there are also many critics that believe that such technologies will exacerbate these and other privacy-related issues for four reasons. First, wide-scale deployment of tiny sensors, coupled with improvements in recognition and data mining algorithms, is allowing personal data to be invisibly captured and analyzed. For example, in January 2001, cameras were used to scan the faces of people at the NFL

- *“Privacy is an interaction, in which the information rights of different parties collide. The issue is of control over information flow by parties that have different preferences over ‘information permeability’.”* ~ Eli Noam

Ubiquities Computing Privacy Issues

1. Data invisibly captured and analyzed
2. Breaking down existing physical and social boundaries in local settings
3. Data accessible at places and times far removed from its original context
4. Easy access to information gathering devices

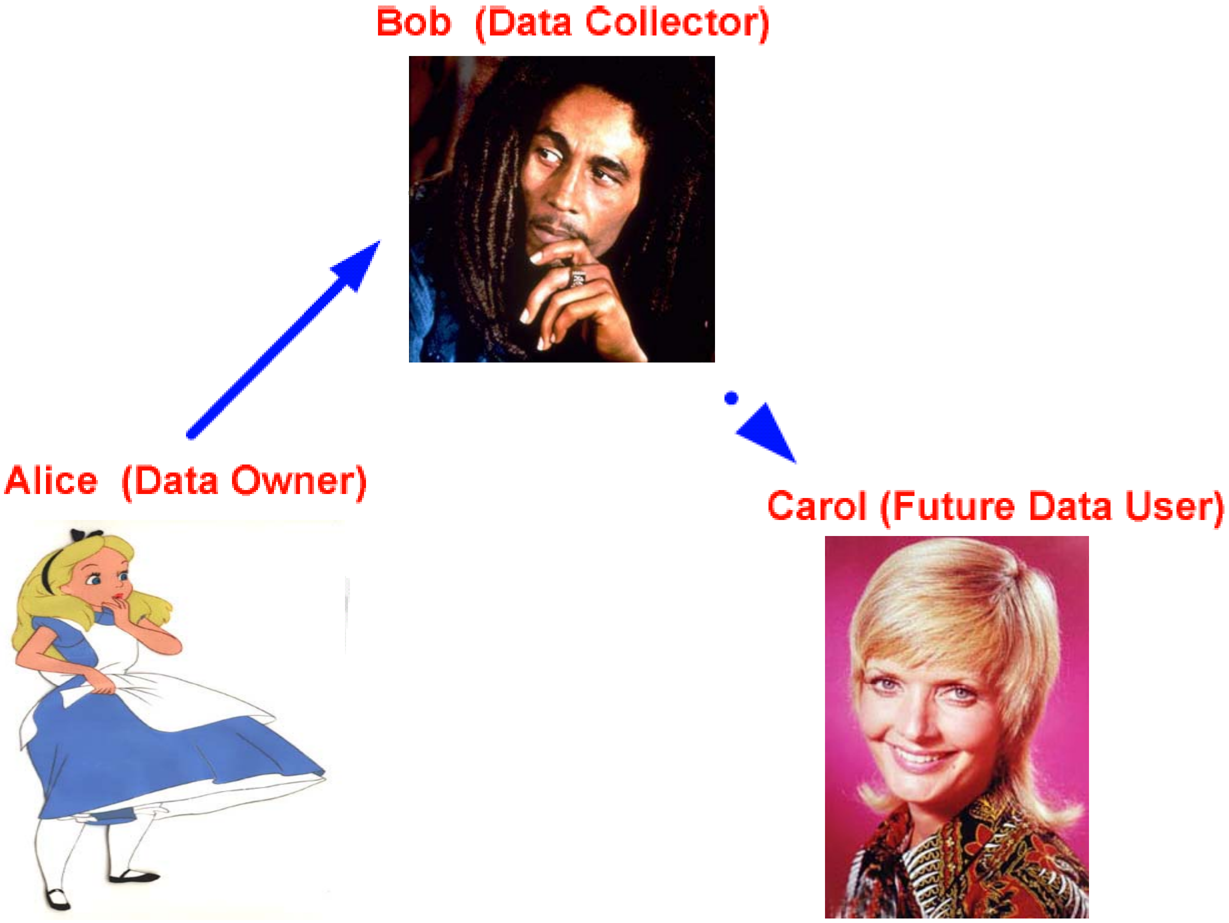
OM-AM

- Objectives, Models, Architectures, and Mechanisms (OM-AM) framework
  - Requirements
    - Objectives and Model
  - How to meet these requirements
    - Architecture and Mechanisms
- Objectives

Asymmetric Information

- Environments with *asymmetric information* describe situations in which some actors hold private information that is relevant to everyone.
- Effect on market
  - Positive
  - Negative

Asymmetric Information

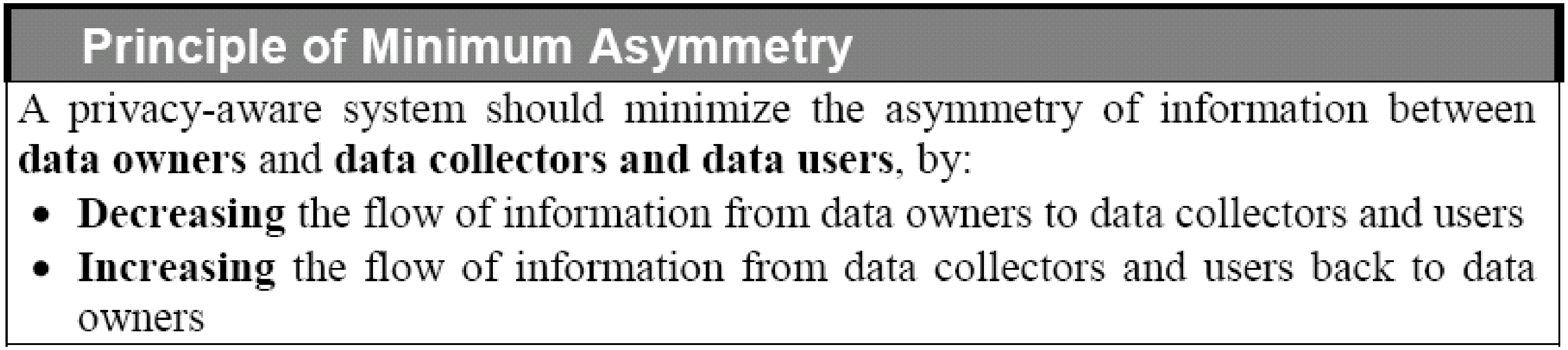


Bob (Data Collector)

Alice (Data Owner)

Carol (Future Data User)

Principle of Minimum Asymmetry

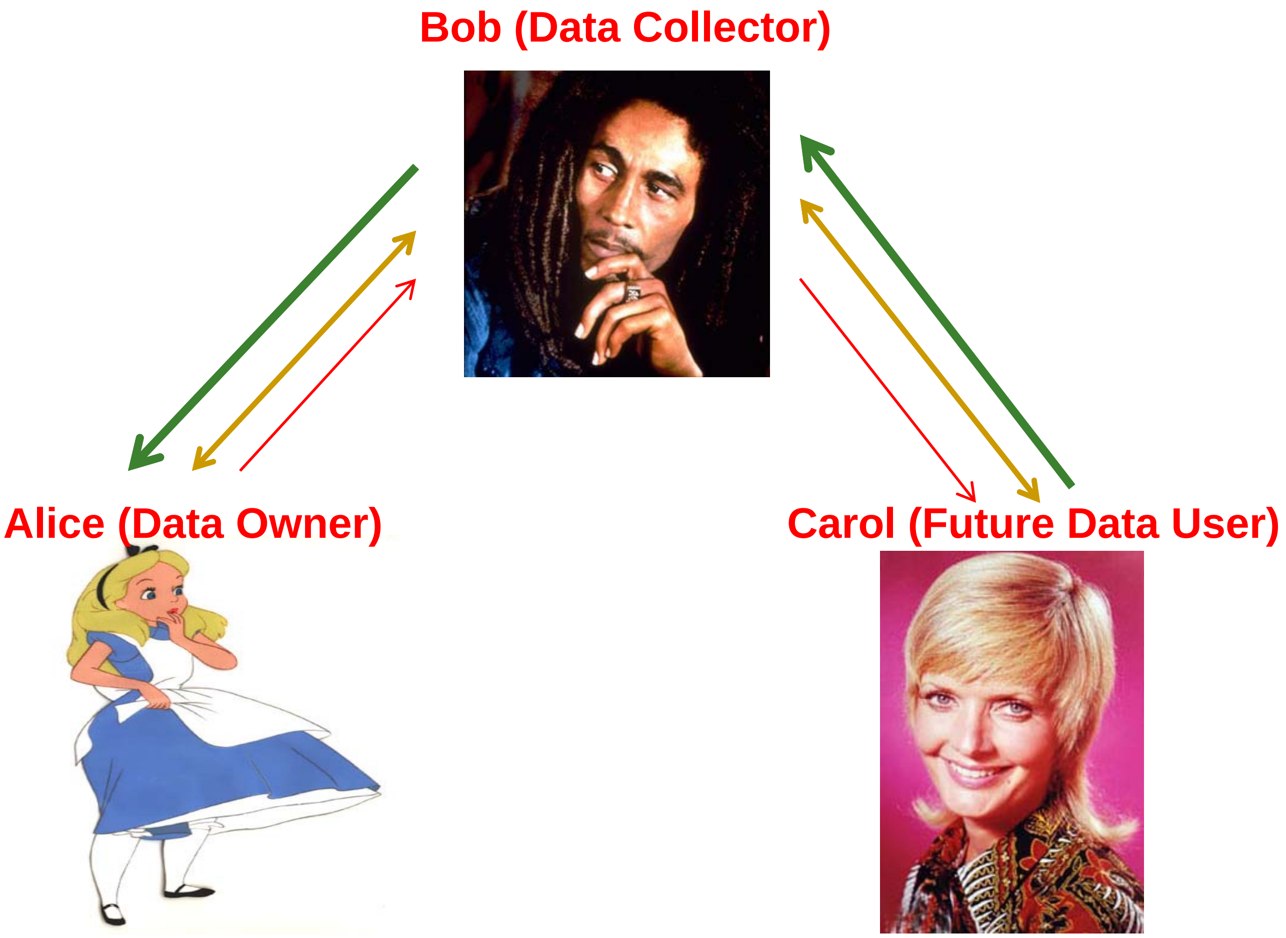


Principle of Minimum Asymmetry

A privacy-aware system should minimize the asymmetry of information between **data owners** and **data collectors and data users**, by:

- **Decreasing** the flow of information from data owners to data collectors and users
- **Increasing** the flow of information from data collectors and users back to data owners

Principle of Minimum Asymmetry



Bob (Data Collector)

Alice (Data Owner)

Carol (Future Data User)

Principle of Minimum Asymmetry

- Market Forces
- Social Forces
- Legal Forces

AIF

- *Approximate Information Flow (AIF)*
  - *Information Space*
  - *Data Lifecycle*
  - *Themes for Minimizing Asymmetry*

Information Space

- Principals
  - Persistence of data
  - Observational accuracy of data
  - Observational confidence of data
- Boundaries
  - Physical boundaries
  - Social boundaries
  - Activity-based boundaries

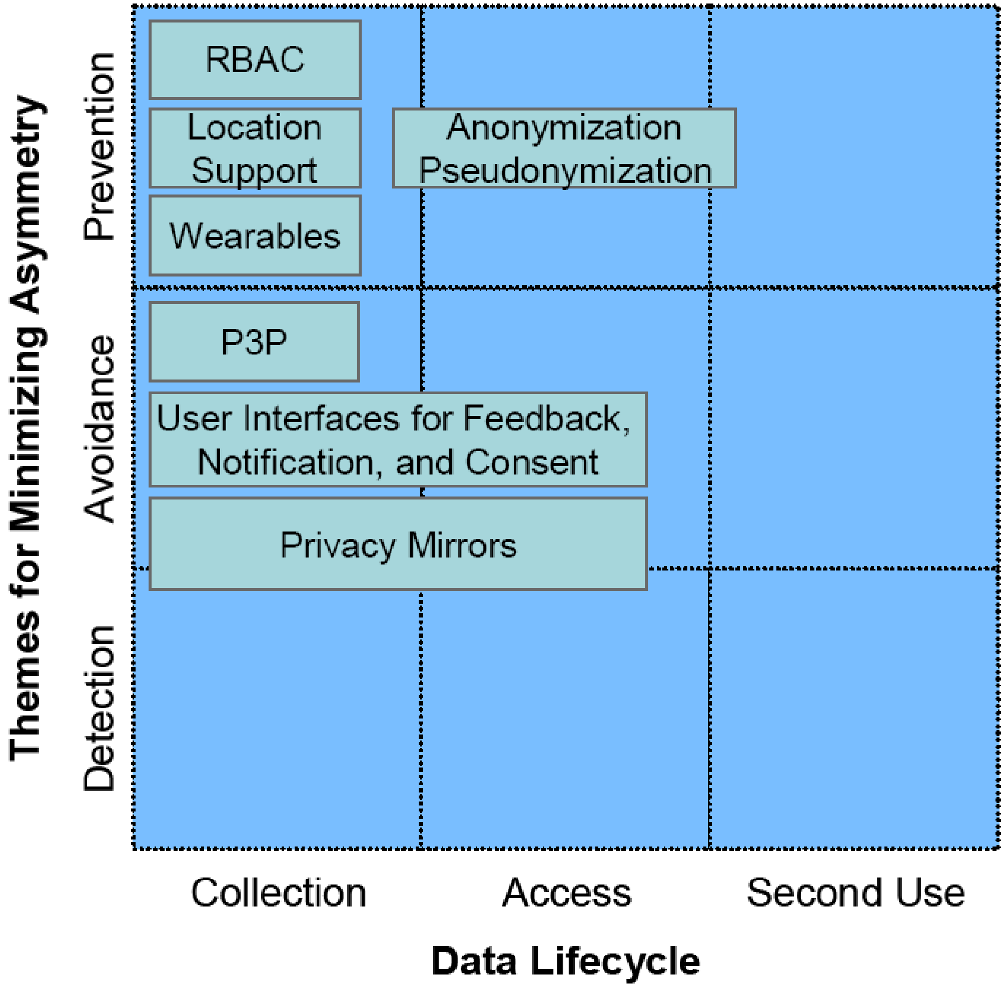
Data Lifecycle

- Collection
  - the point at which data is gathered
- Access
  - the point at which data is initially requested
- Second use
  - use and sharing of data after initial access has been made

Themes for Minimizing Asymmetry

- Prevention
  - seeks to ensure that undesirable use of private data will not occur
- Avoidance
  - carefully considering the context in which data exchange takes place
- Detection
  - assumes that some undesirable use will occur, and seeks to find such incidents in the hope that privacy violators will be held accountable

Design Space of Privacy Solutions



Themes for Minimizing Asymmetry

Prevention

Avoidance

Detection

RBAC

Location Support

Wearables

Anonymization Pseudonymization

P3P

User Interfaces for Feedback, Notification, and Consent

Privacy Mirrors

Collection

Access

Second Use

Data Lifecycle

Contributions

- The AIF model useful for analyzing tools.
- The idea the minimizing asymmetry is good for all parties involved.
- Using AIF to certify products.

Discussion

- Would it be to difficult to move from the asymmetric information flow model we have now?
- Could this be legally enforced?