



# **Privacy Support for Users Beyond Transparency and Control**

**Alfred Kobsa**

Donald Bren School of Information and Computer Sciences  
University of California, Irvine



# 2012 White Paper on U.S. Consumer Privacy Bill of Rights

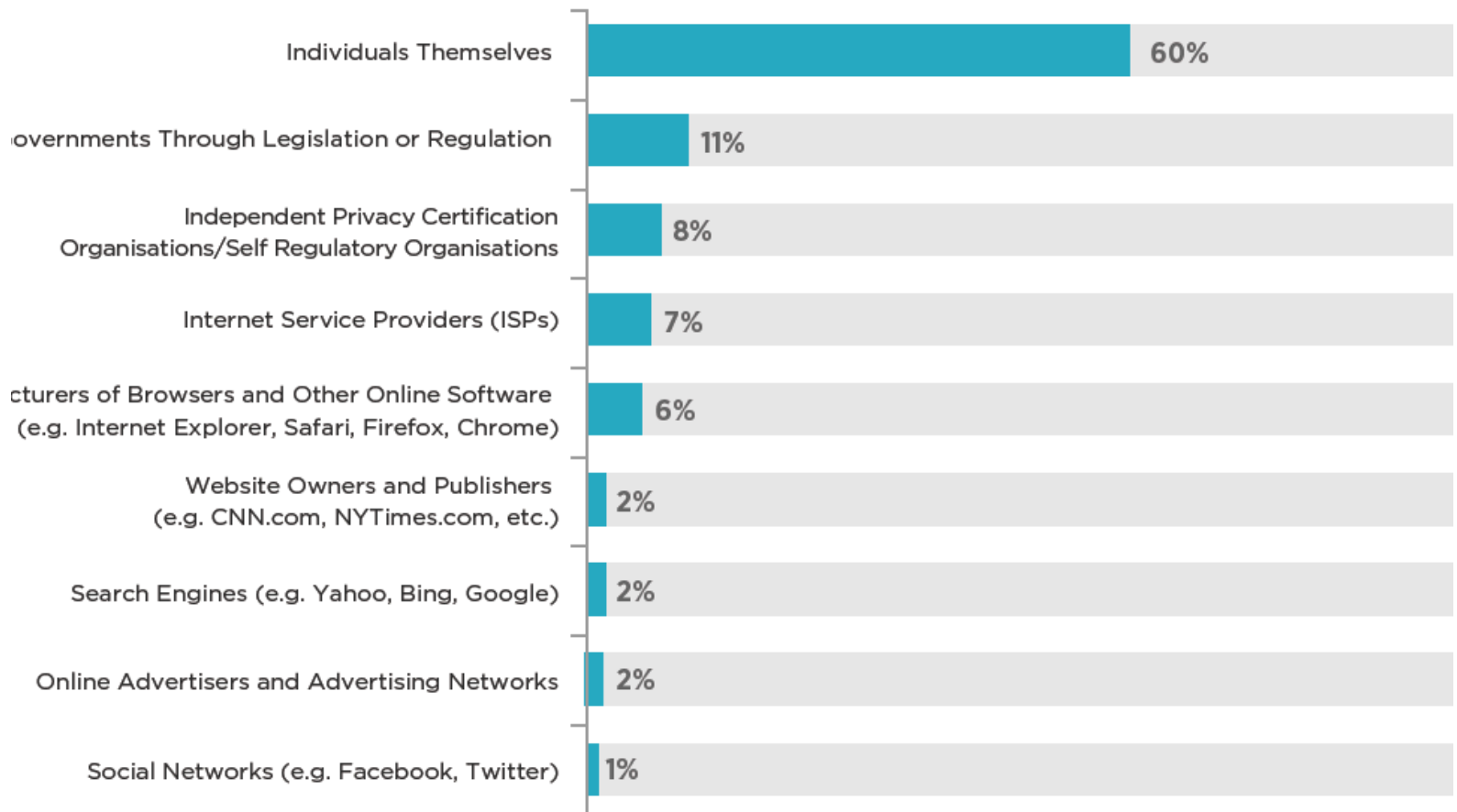
**Individual Control:** users get right to exercise control over what personal data companies collect from them and how they use it. Companies should offer consumers *clear and simple choices*, *presented at times and in ways that enable consumers to make meaningful decisions* about personal data collection, use, and disclosure

**Transparency:** users get right to easily understandable and accessible information about privacy / security practices

Companies should provide clear descriptions of [...] why they need the data, how they will use it

# People trust themselves the most in protecting their privacy

## WHO CONSUMERS TRUST THE MOST TO PROTECT THEIR PRIVACY



TRUSTe 2012 (Great Britain)

# Facebook Privacy Settings

(transparency, control, choice)

## Choose Your Privacy Settings ▶ Applications, Games and Websites

[◀ Back to Privacy](#)

Applications you u

Info accessible th  
friends

Game and applica  
activity

Instant personaliz

Public search

### Info accessible through your friends

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

<input type="checkbox"/> Bio	<input type="checkbox"/> My videos
<input type="checkbox"/> Birthday	<input type="checkbox"/> My links
<input type="checkbox"/> Family and relationships	<input type="checkbox"/> My notes
<input type="checkbox"/> Interested in and looking for	<input type="checkbox"/> Photos and videos I'm tagged in
<input type="checkbox"/> Religious and political views	<input type="checkbox"/> Hometown
<input type="checkbox"/> My website	<input type="checkbox"/> Current city
<input type="checkbox"/> If I'm online	<input type="checkbox"/> Education and work
<input type="checkbox"/> My status updates	<input type="checkbox"/> Activities, interests, things I like
<input type="checkbox"/> My photos	<input type="checkbox"/> Places I check in to

Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.

[Save Changes](#) [Cancel](#)

Show a preview of your Facebook profile when people look for you using a search engine.

[Edit Settings](#)

# Transparency and control can become unwieldy

Facebook has

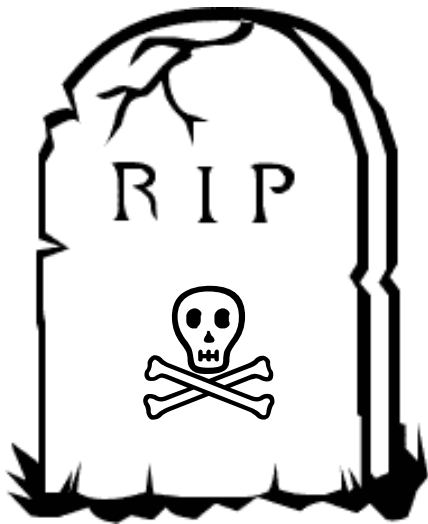
- “bewildering tangle of options” (New York Times, 2010)
- “labyrinthian” controls” (U.S. Consumer Magazine, 2012)
- Liu et al. (2011): 63% of the photos of Facebook users had privacy settings that were inconsistent with users’ desired settings.
- Madejski et al. (2012): every subject had at least one item whose actual disclosure did not match the subject’s disclosure intentions.

# People are not rational privacy decision makers

*Weighing immediate benefits against possible unknown risks sometimes in the future is very difficult*

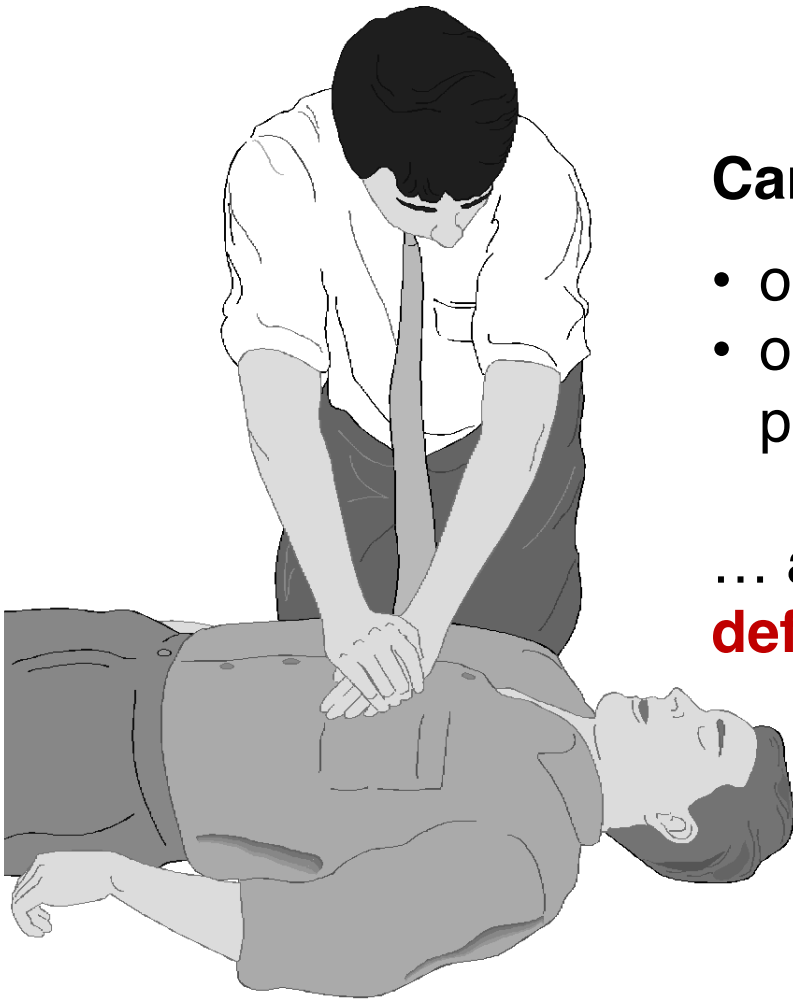
- Herding effect on disclosure (Acquisti et al. 2011)
- Order effect on disclosure (Acquisti et al. 2011)
- Privacy information raises privacy fears (Knijnenburg et al. 2012)
- If misplaced in the workflow, privacy notices become ignored (Egelman et al. 2009)
- Professionalism of UI design matters (John et al. 2011)
- Interface elements influence disclosure rate (Groom & Calo 2011)
- It matters what the default is and how one asks (Lai & Hui 2006)
- Control may lead to over-disclosure (Brandlmarte et al. 2012)

# The Death of Transparency and Control?



- **“Transparency-and-choice has failed”**  
[Nissenbaum 2011]
- **It does not “provide people with meaningful control over their data”** [Solove 2012]
- **Notice and control is a “red herring”**  
[Barocas & Nissenbaum 2009]
- **Transparency is a “sleight of privacy”**  
[Adjerid et al. 2013]
- **Big data is the “death knell for informed consent”** [Barocas & Nissenbaum 2013]

# Or, is there still hope?



**Can we re-orient transparency and control**

- onto the **important** privacy decisions only?
- onto people who **want** to self-manage privacy?

... and have **suitable personalized privacy defaults** for all remaining privacy decisions?



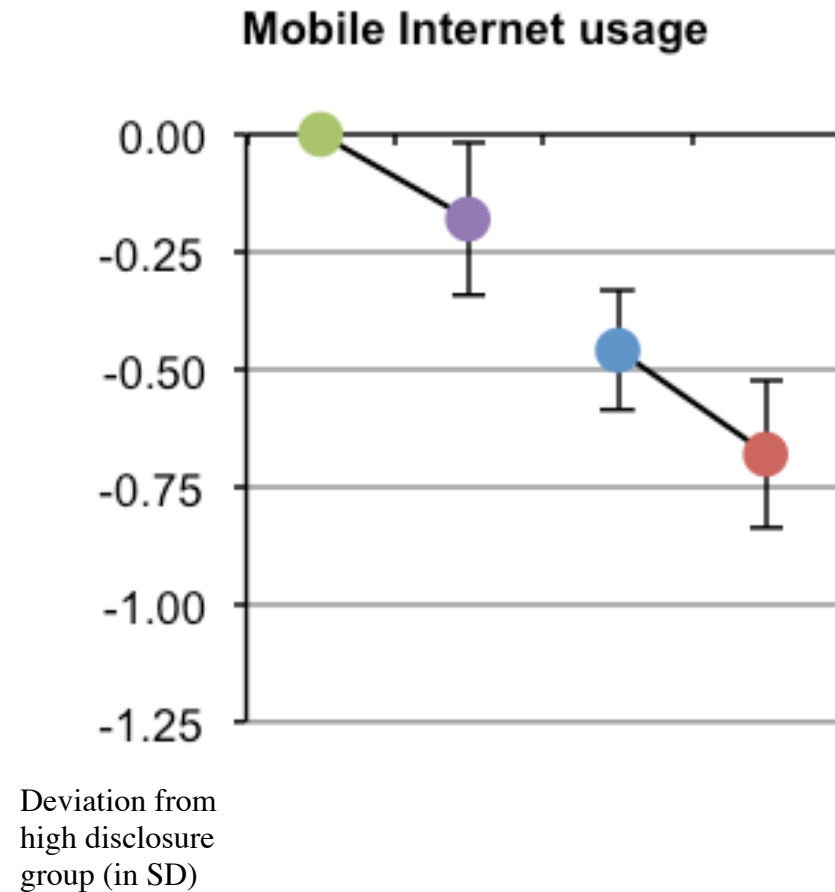
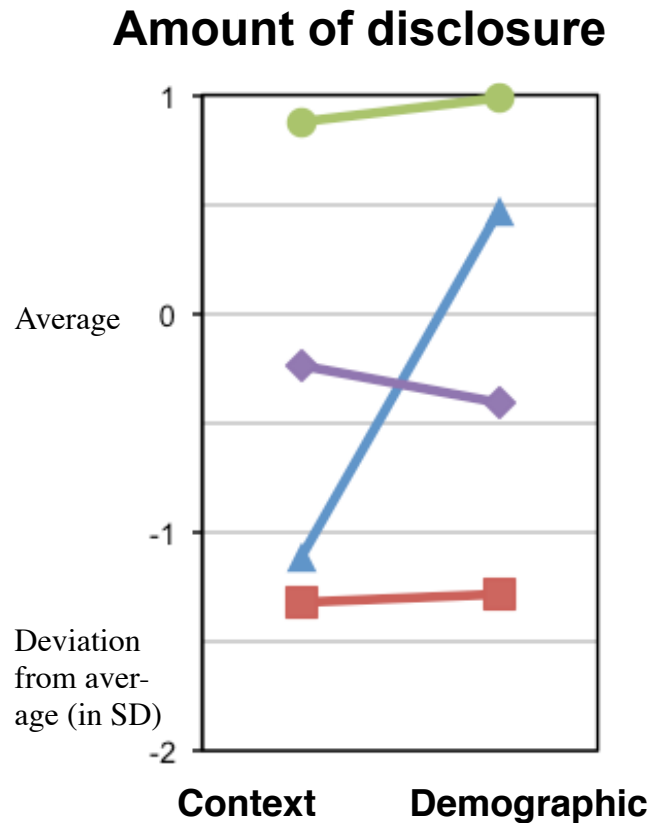
# Proposed solution

1. **\*Predict\*** what privacy decisions would be consistent with users' preferences
2. Make this decision on behalf of users (e.g., via **personalized privacy default settings**)
3. allow that users **inspect and override some or all predictions**
4. record any corrections by the user, and **modify prediction algorithm over time**

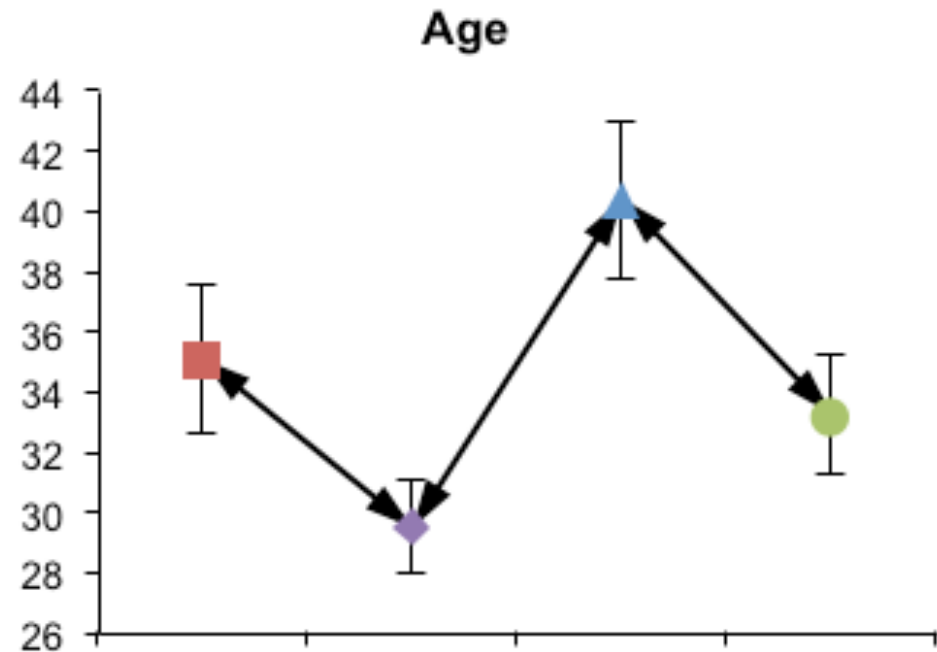
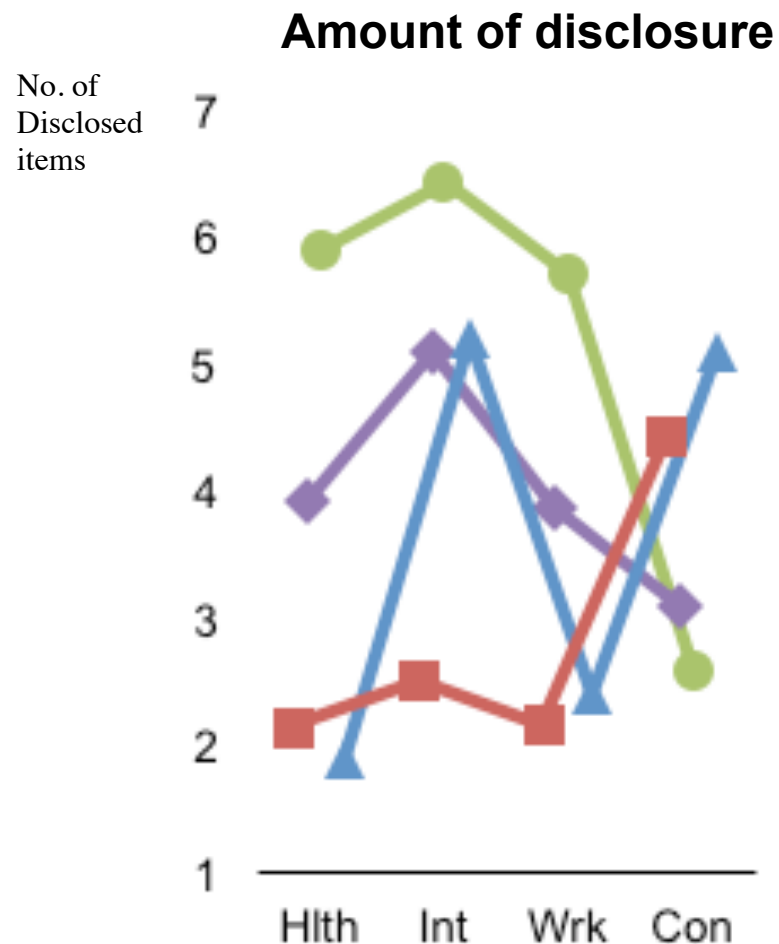
## Three lines of work

- Assignment of users to **privacy clusters**
- **Individual prediction**
- **Privacy control without a UI**  
(e.g., in the “Internet of Things”, “sensor environments”)

# User clusters based on the disclosure of context and demographic data

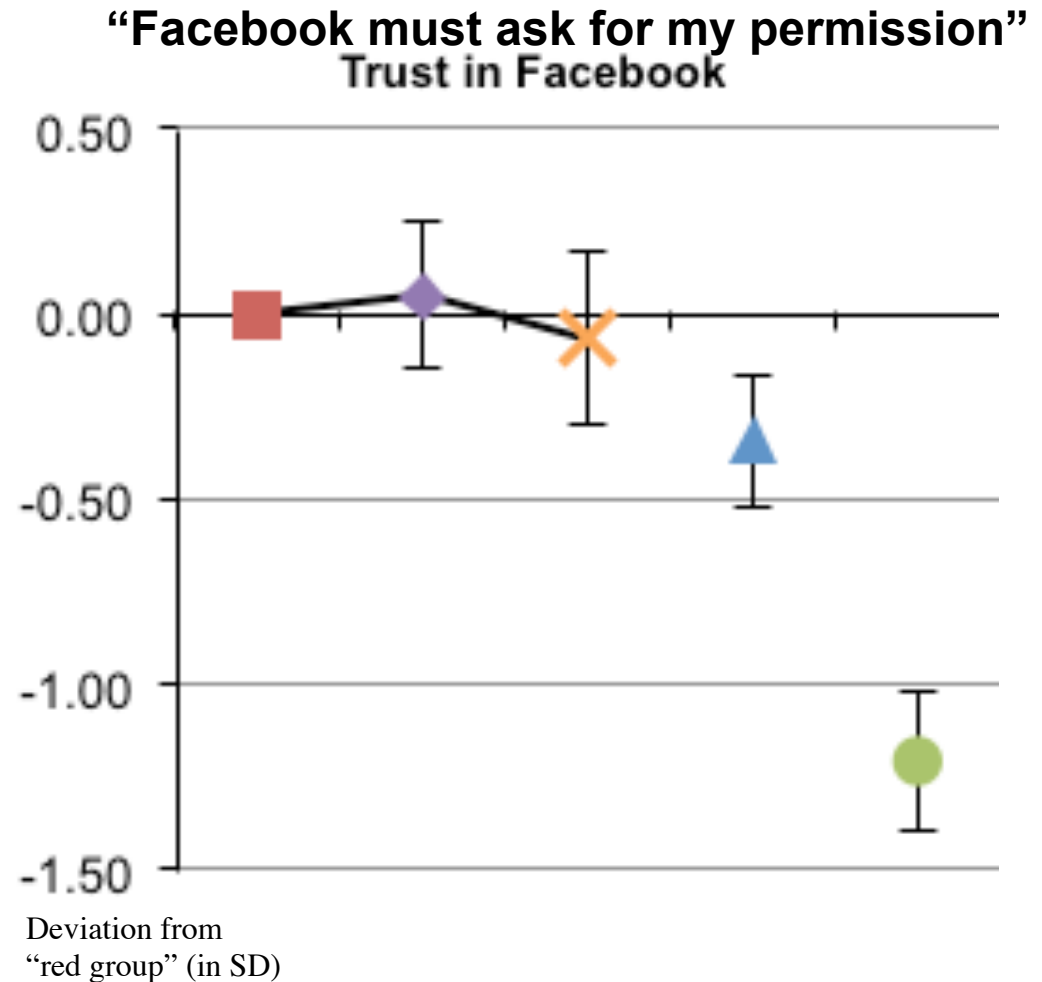
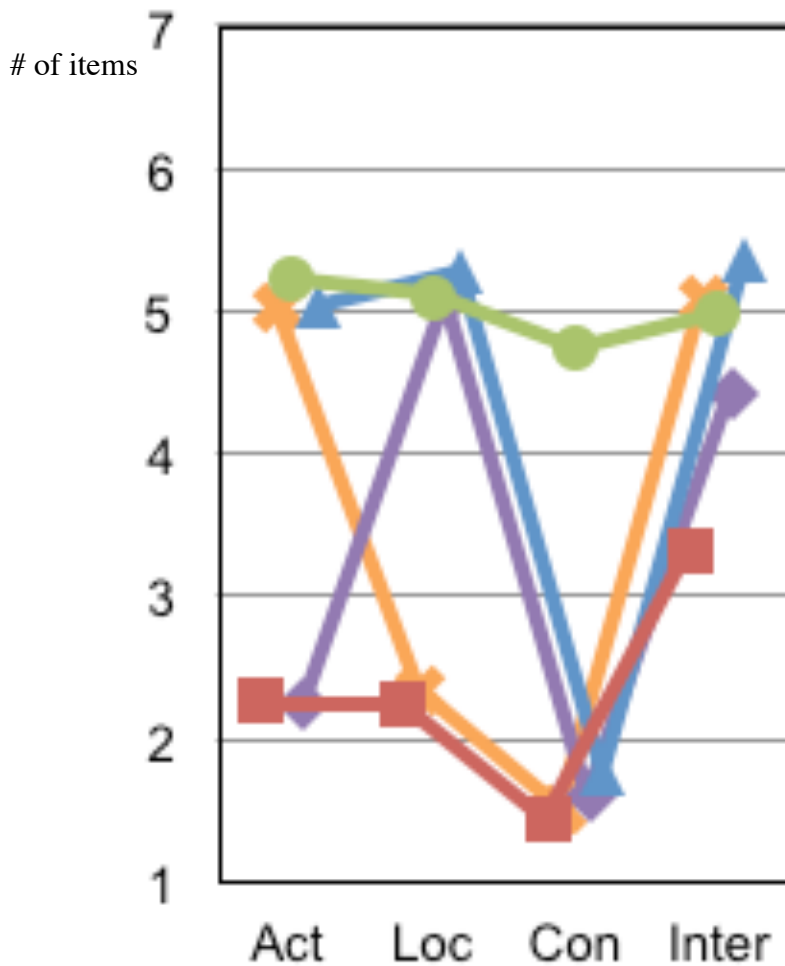


# User clusters based on the likelihood-to-disclose personal data to an online retailer



# User clusters based on the disclosure of four types of Facebook data

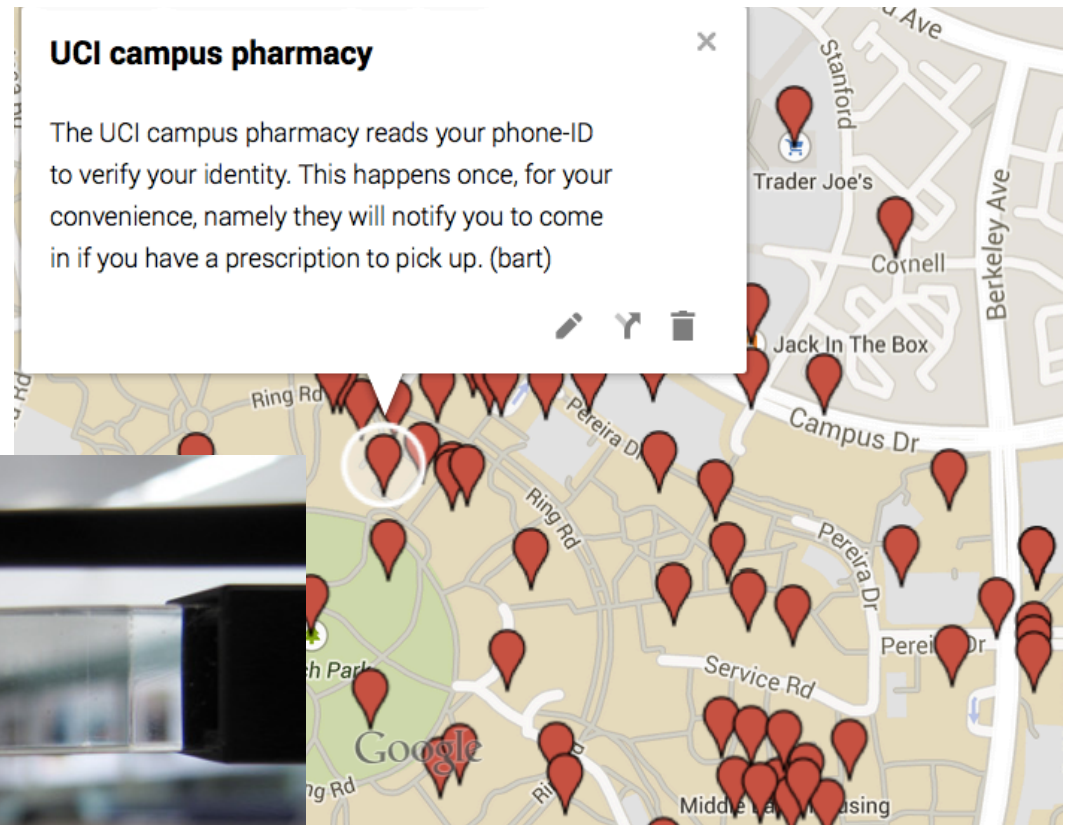
## Level of intention-to-disclose



# Individual prediction

- **Based on “static” data about users**
  - Data from privacy survey in 8 countries on 4 continents
  - 9,625 participants
  - Analyzing influence on the prediction of privacy decisions:
    1. Cultural values (Schwartz) or dimensions (Hofstede)
    2. Context, privacy attitudes
    3. Demographics
- **Based on past disclosures**
  - CMU: prediction of location disclosure

# Privacy w/o an interface in the Internet of Things



# Privacy w/o an interface in the Internet of Things




- Privacy impact assessment  
(templates from DHS, NIST, Canada, Germany)
- Stakeholder interviews
- “Interface-less” privacy control



# Consumer Privacy Bill of Rights Act of 2015

Individual Control: mechanisms that are reasonably accessible, understandable, and usable

-  Industry needs to conduct research on *privacy decision support* for each application that collects personal data:
- **During user needs analysis and early usability testing:**  
Run user studies and identify groups with different disclosure behaviors, and characteristics that predict these groups (age, gender, internet use).
  - **In regular intervals:**  
Rerun user studies and re-verify the utility of privacy decision support