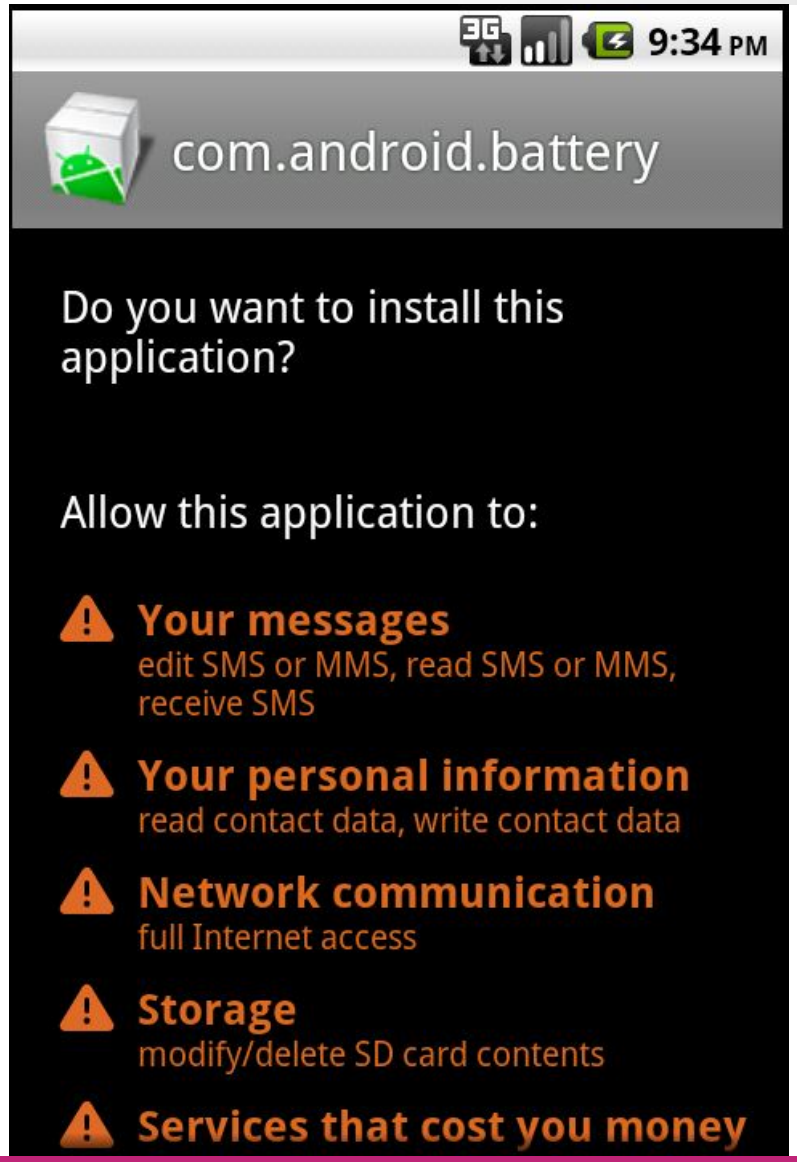
Towards personalized privacy defaults

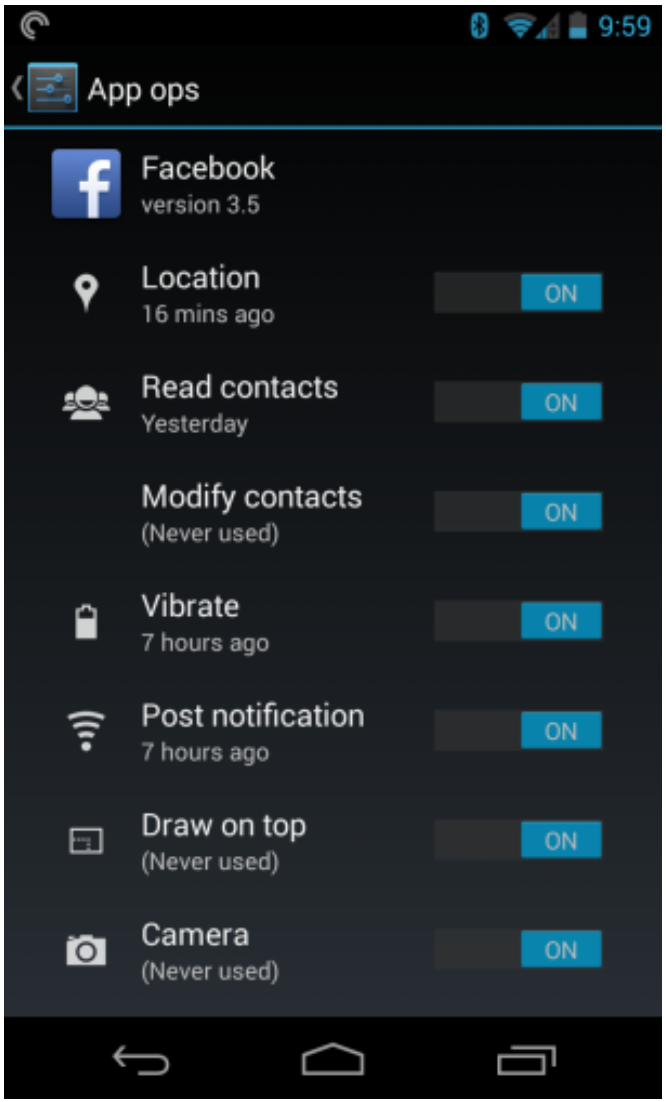
Alfred Kobsa

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

Privacy permissions: Take it or leave it



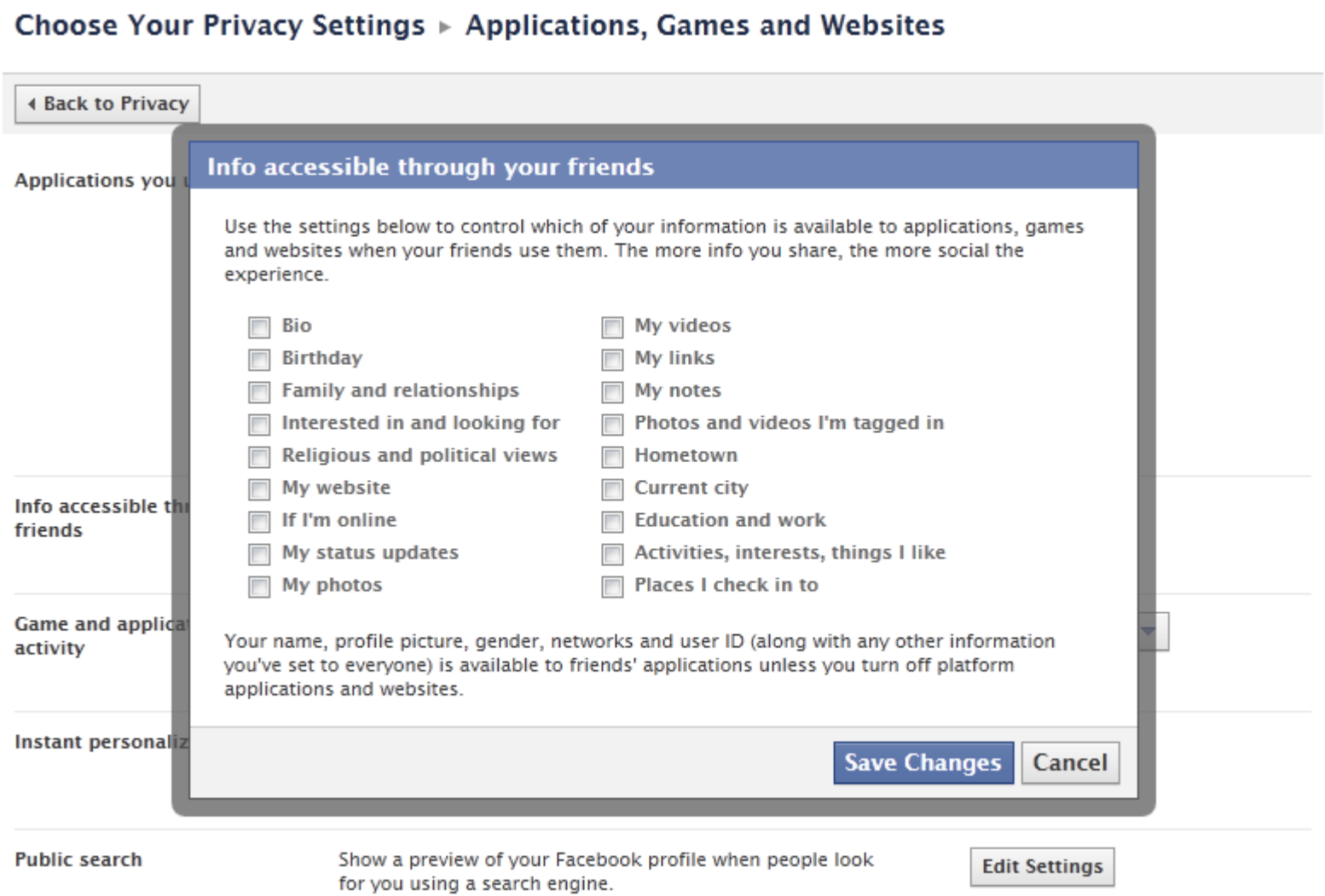
Transparency! Control! Choice!



Android, Windows Phone:

Information about and control over every permission

Facebook Privacy Settings
(more transparency, control, choice!)



Principles from the proposed U.S. Consumer Privacy Bill of Rights (2012)

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

Industry is asked to develop a code of conduct that will be enforced by the U.S. Federal Trade Commission

Proposed General Data Protection Regulation of the European Commission

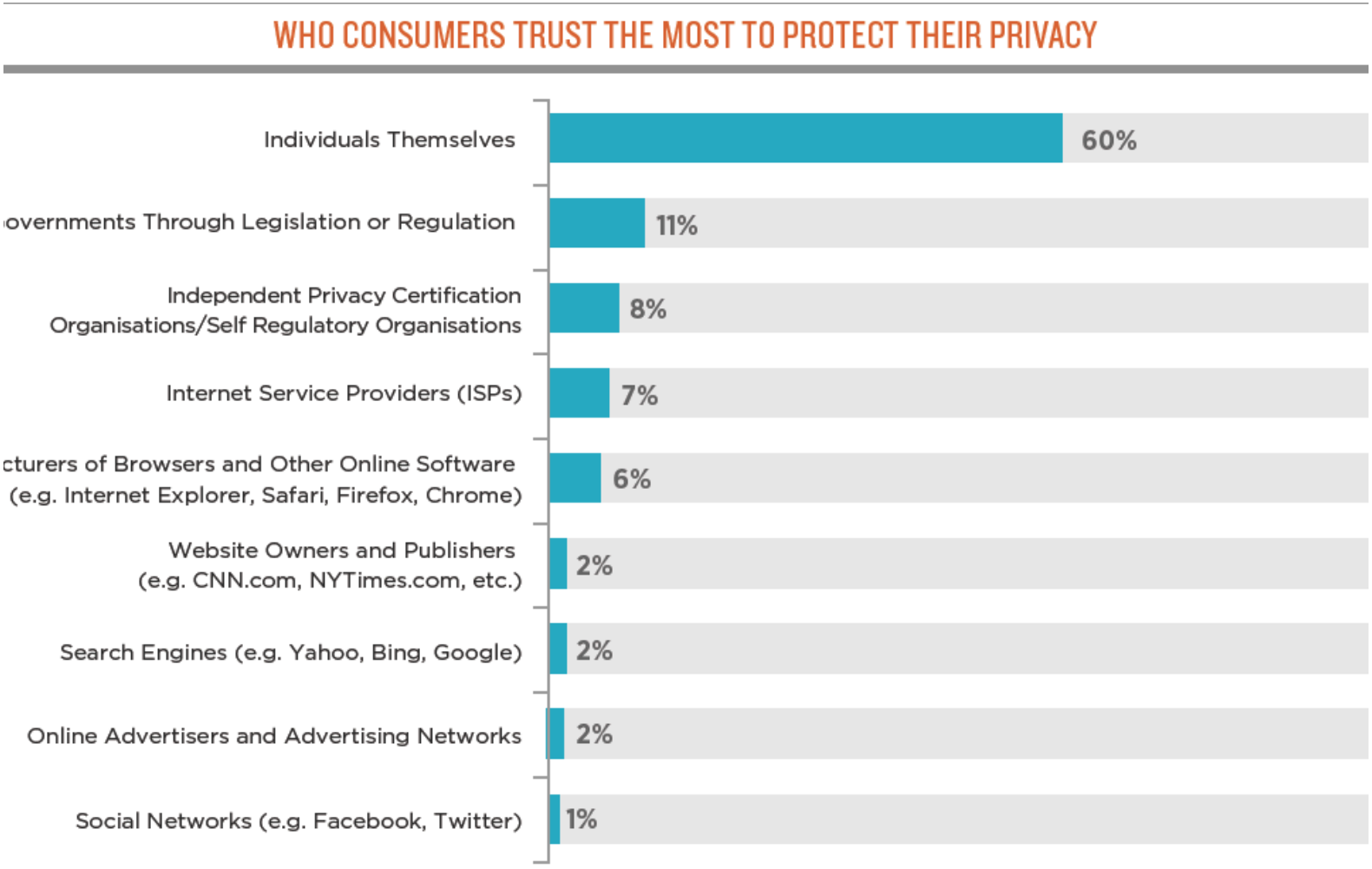
Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

a.the data subject has given consent to the processing of their personal data for one or more specific purposes

- The information in relation to the processing of personal data […] should be given to them *at the time of collection*
- The controller shall provide any information […] in *an intelligible form, using clear and plain language, adapted to the data subject*

Applies to data processors worldwide who offer goods or services to European Union residents or monitor their behavior

People trust themselves the most in protecting their privacy



TRUSTe 2012 (Great Britain)

Data disclosure decisions 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

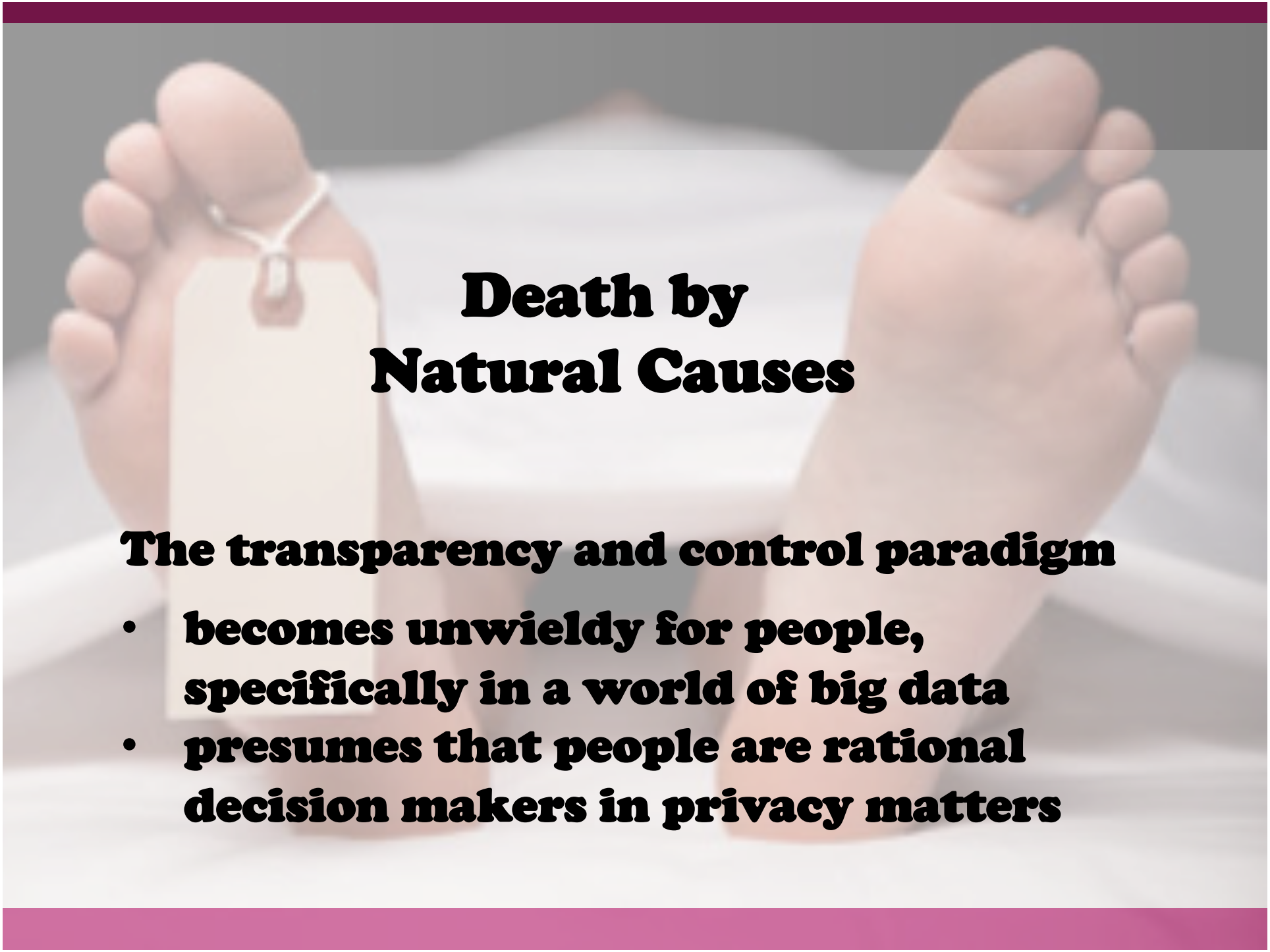
- Herding effect on disclosure (Acquist
- Order effect on disclosure (Acquisti e
- Privacy information raises privacy f l. 2012)
- If misplaced in the workflow, privacy gnored (Egelman et al. 2009)
- Professionalism of UI design matte
- Interface elements influence disclosure rate (Groom & Calo 2011)
- 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]

President's Council of Advisors on Science and Technology

- "The framework of notice and consent is […] becoming unworkable as a useful foundation for policy."
- "The conceptual problem with notice and consent is that it fundamentally places the burden of privacy protection on the individual."
- "Notice and consent creates a non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer. This is a kind of market failure."

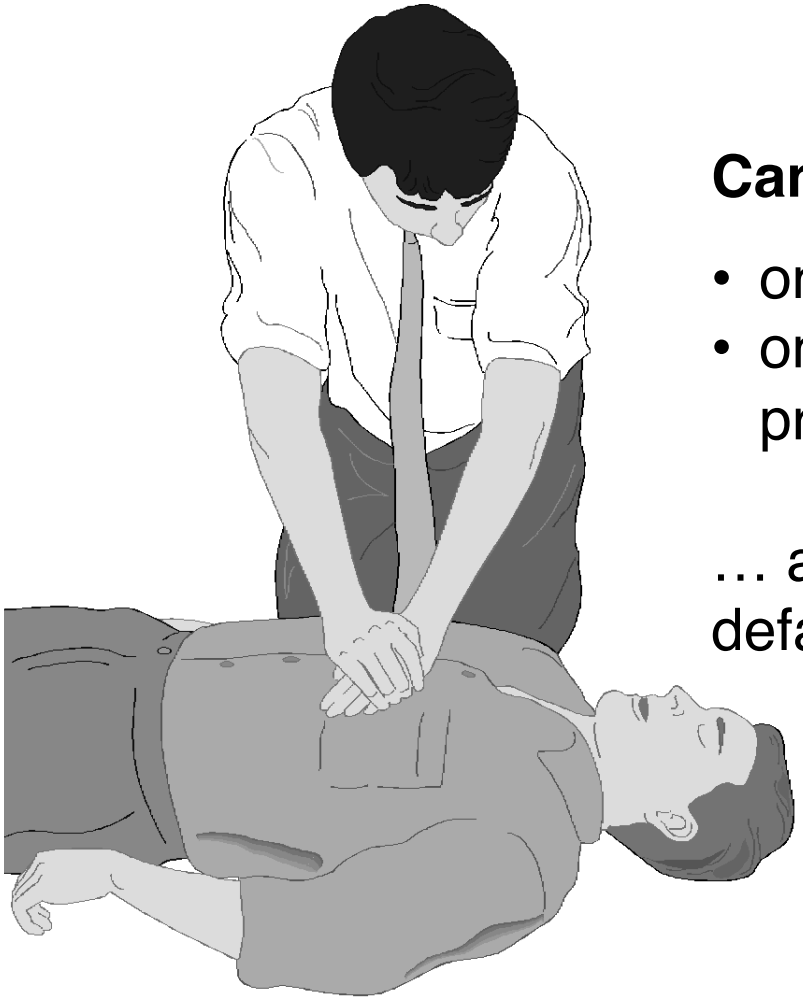


Death by Natural Causes

The transparency and control paradigm

- **becomes unwieldy for people, specifically in a world of big data**
- **presumes that people are rational decision makers in privacy matters**

Or, is there still hope?



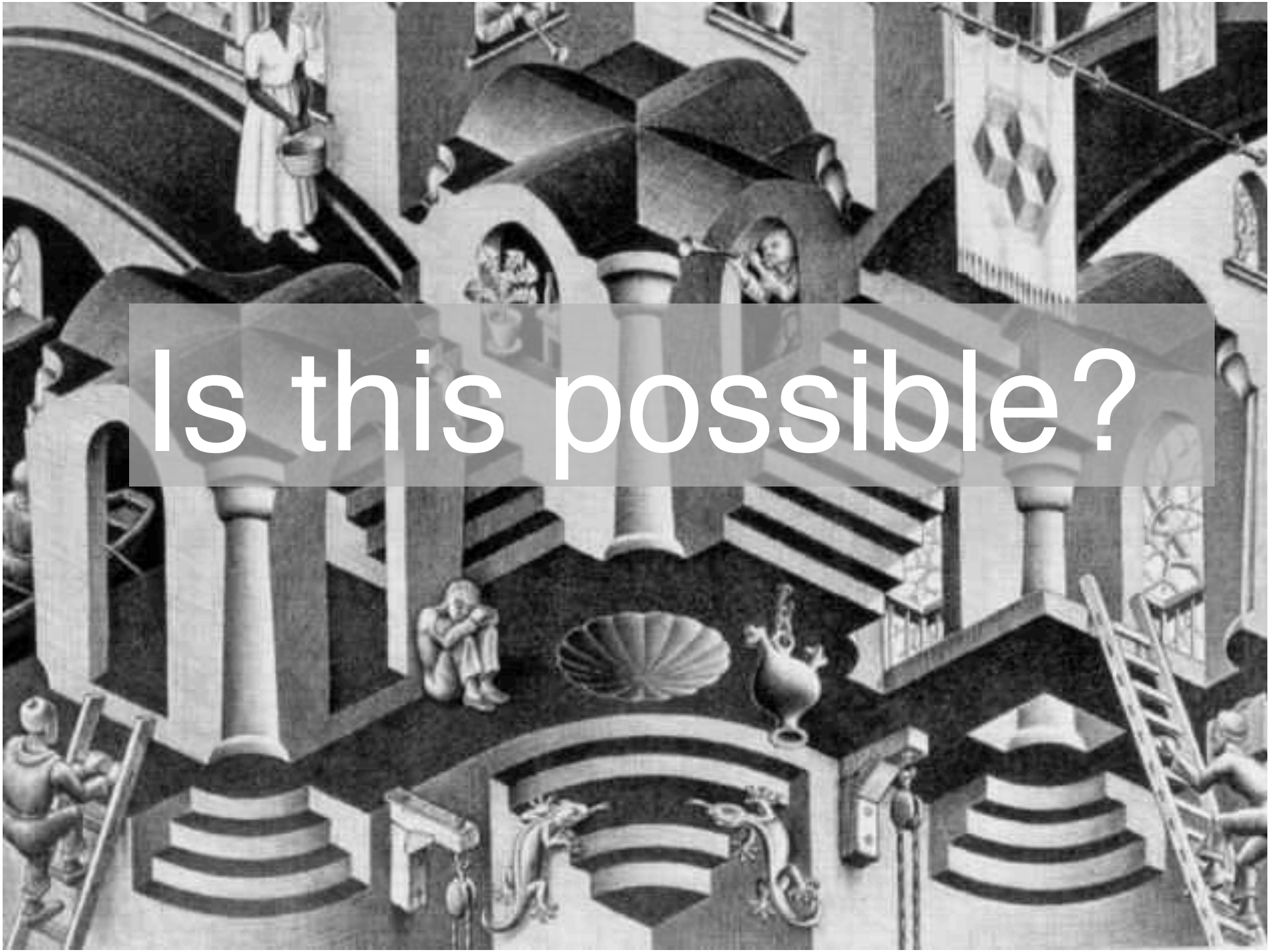
Can we re-orient transparency and control

- 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

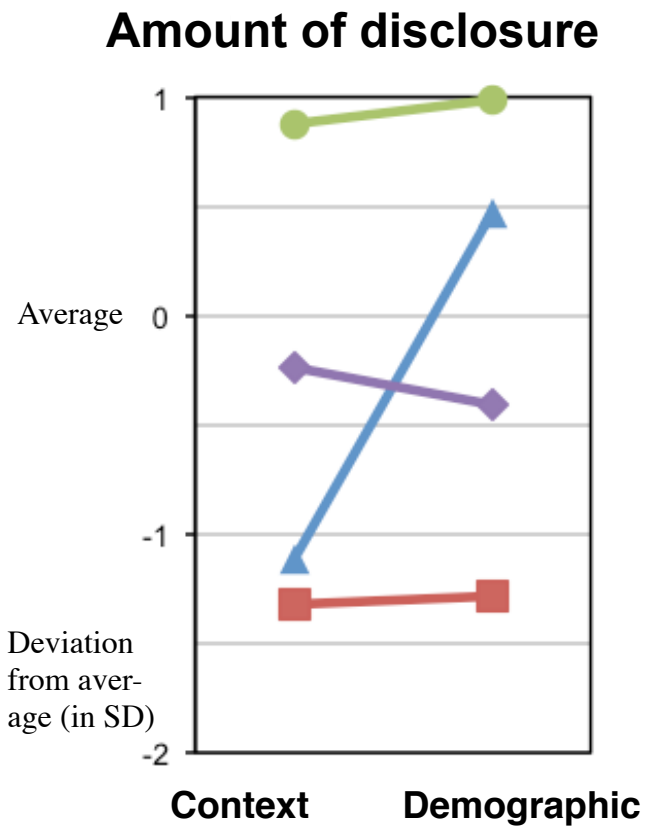
1. *__Predict__* what privacy decisions would be consistent with users' preferences
2. Make this decision **on behalf of users** (e.g., via **personalized privacy default settings**)
3. allow that users **override** some or all predictions
4. record any corrections by the user, and **modify prediction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

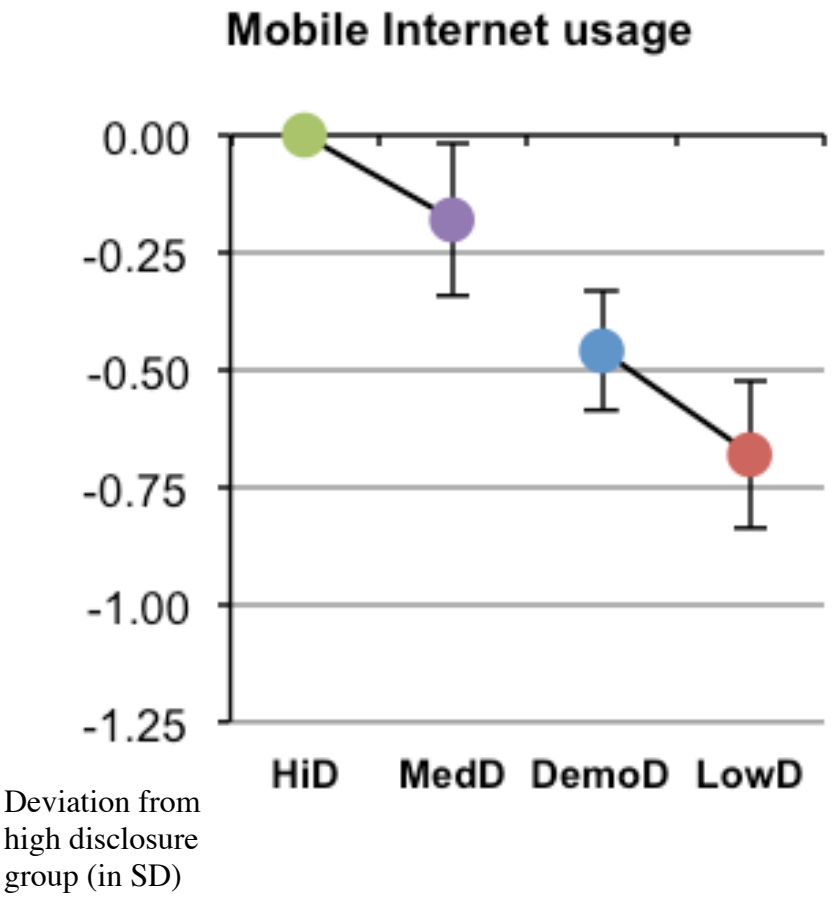

Is this possible?

Disclosure data from three experiments

- Asked participants about various personal data
- Recorded whether or not they disclosed them
- Performed factor analysis to determine types of personal data for which subjects showed similar disclosure behavior
- Performed cluster analysis to find subgroups of subjects with similar disclosure behavior

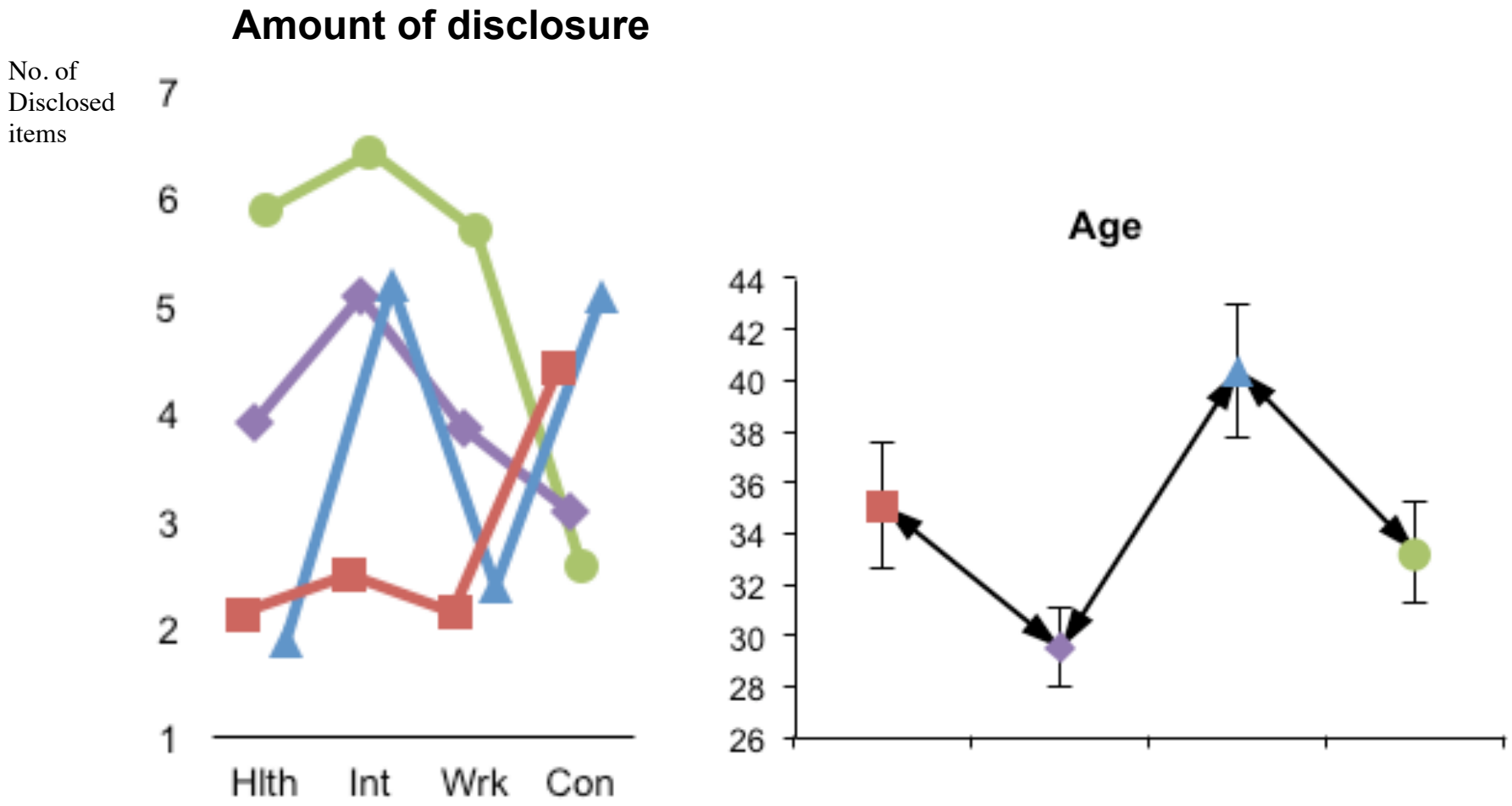
User clusters based on the disclosure of context and demographic data





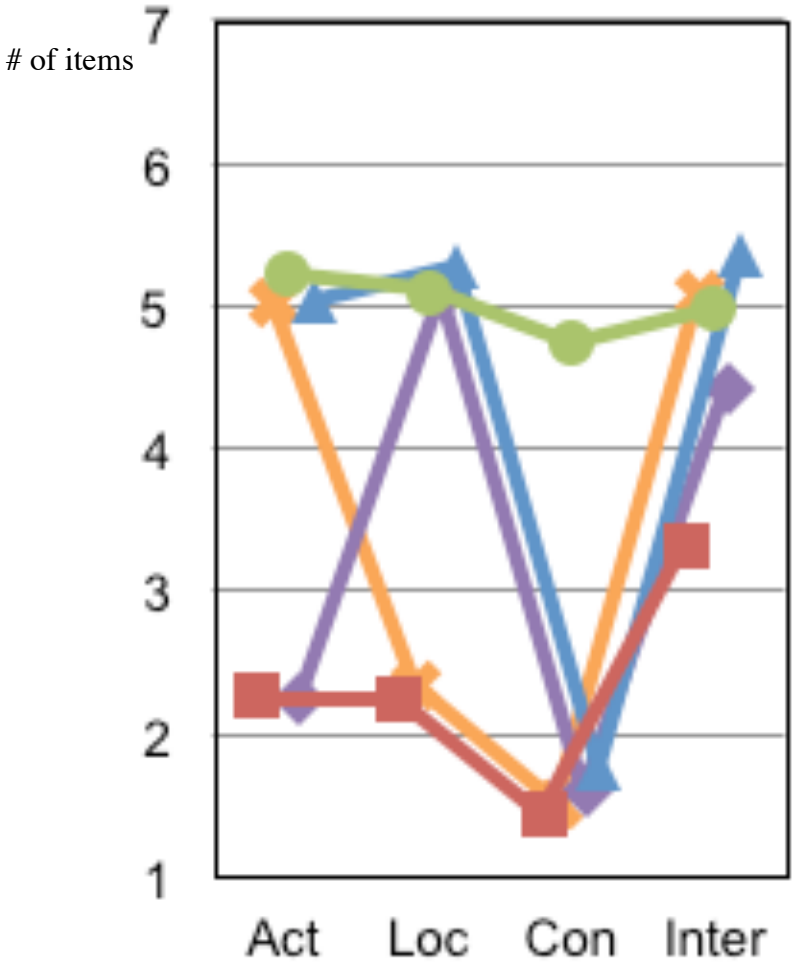
Knijnenburg, Kobsa & Jin *IJHCS* (2013)

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

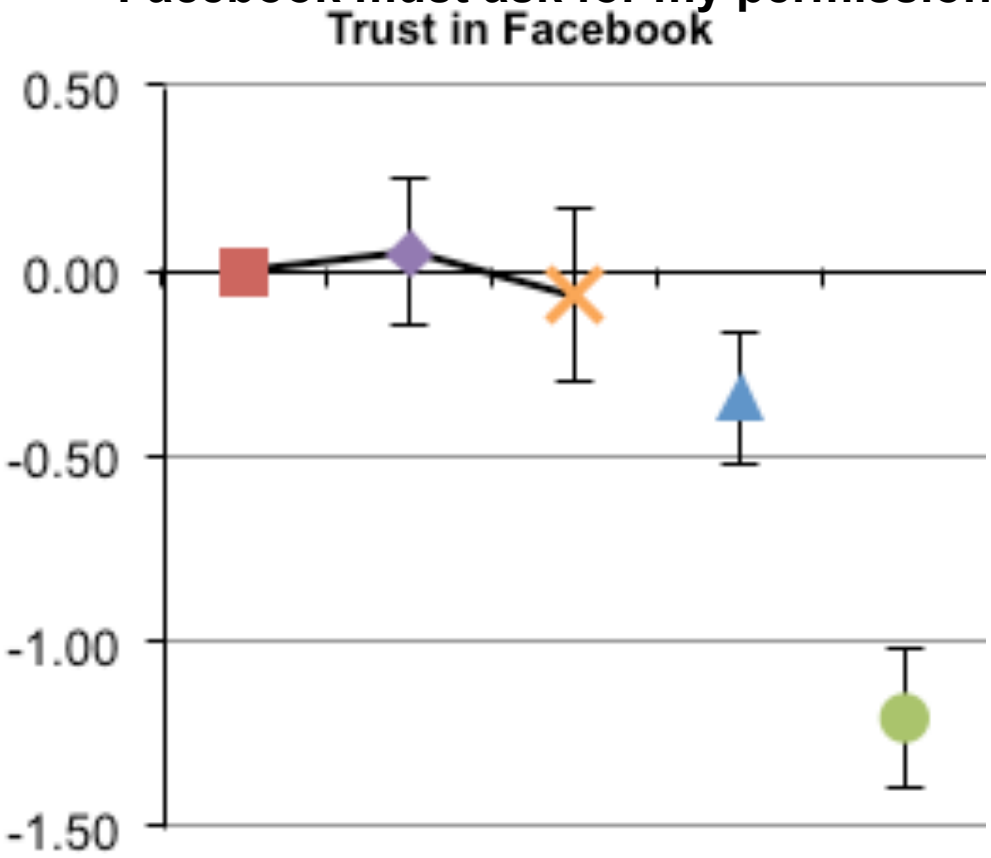


User clusters based on the disclosure of four types of Facebook data

Level of intention-to-disclose



"Facebook must ask for my permission"



Industry needs to conduct research on *privacy decision support* for each product 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).

At runtime:

1. Determine a user's characteristics (age, gender, ….)
2. Predict the user's privacy group based thereon, with associated predicted privacy behavior
3. Cater to this anticipated behavior
   - Set default privacy preferences for the user
   - Adjust privacy-related information

In regular intervals:

Rerun user studies and re-verify the utility of privacy decision support

Alternative machine-learning solution

During user needs analysis and early usability testing:

Run user studies and identify groups with different disclosure behaviors, and other characteristics of these groups (age, gender, internet usage).

At runtime:

1. Determine a user's characteristics (age, gender, ….)
2. Predict the user's privacy group based thereon, with associated predicted privacy behavior
3. Cater to this anticipated behavior
   - Set default privacy preferences for the user
   - Adjust privacy-related information

In regular intervals:

Rerun user studies and re-verify the utility of privacy decision support

New directions for privacy regulation

Require that data collectors

- conduct studies on privacy decision behaviors of data subjects
- based thereon, provide *privacy decision support* to data subjects (rather than merely posting privacy statements or offering fine-grained privacy choices)
- publish the results and consequences drawn, and collaborate on industry-wide solutions
- re-verify the usefulness of their privacy decision support in regular intervals
- follow best practices in their research, and be accountable for what they do