Privacy Support for Users
Beyond Transparency and Control

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

<table>
<thead>
<tr>
<th>Trust Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals Themselves</td>
<td>60%</td>
</tr>
<tr>
<td>Governments Through Legislation or Regulation</td>
<td>11%</td>
</tr>
<tr>
<td>Independent Privacy Certification Organisations/Self Regulatory Organisations</td>
<td>8%</td>
</tr>
<tr>
<td>Internet Service Providers (ISPs)</td>
<td>7%</td>
</tr>
<tr>
<td>Makers of Browsers and Other Online Software (e.g., Internet Explorer, Safari, Firefox, Chrome)</td>
<td>6%</td>
</tr>
<tr>
<td>Website Owners and Publishers (e.g., CNN.com, NYTimes.com, etc.)</td>
<td>2%</td>
</tr>
<tr>
<td>Search Engines (e.g., Yahoo, Bing, Google)</td>
<td>2%</td>
</tr>
<tr>
<td>Online Advertisers and Advertising Networks</td>
<td>2%</td>
</tr>
<tr>
<td>Social Networks (e.g., Facebook, Twitter)</td>
<td>1%</td>
</tr>
</tbody>
</table>

TRUSTe 2012 (Great Britain)
Facebook Privacy Settings
(transparency, control, choice)

Choose Your Privacy Settings ➤ Applications, Games and Websites

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.

- Bio
- Birthday
- Family and relationships
- Interested in and looking for
- Religious and political views
- My website
- If I'm online
- My status updates
- My photos

- My videos
- My links
- My notes
- Photos and videos I'm tagged in
- Hometown
- Current city
- Education and work
- Activities, interests, things I like
- 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.
Facebook has

- “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

Knijnenburg, Kobsa & Jin *IJHCS* (2013)
User clusters based on the likelihood-to-disclose personal data to an online retailer

Amount of disclosure

No. of Disclosed items

Age

Hlth  Int  Wrk  Con
User clusters based on the disclosure of four types of Facebook data

Level of intention-to-disclose

“Facebook must ask for my permission”

Deviation from “red group” (in SD)
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

UCI campus pharmacy

The UCI campus pharmacy reads your phone-ID to verify your identity. This happens once, for your convenience, namely they will notify you to come in if you have a prescription to pick up. (bart)
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
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