A user-tailored approach to privacy decision support

Bart P. Knijnenburg
@usabart

Slides and more:
usabart.nl
Hello, I’m Bart

bartk@clemson.edu
www.usabart.nl
@usabart

Clemson University (Asst. Prof.)
UC Irvine (PhD)
Carnegie Mellon University (M)
TU Eindhoven (BS + MS)
Past, Present, Future

TU Eindhoven
- Inspectability and Control
- Choice Overload & Diversification
- Preference Elicitation
- User-Centric Evaluation

UC Irvine
- User-Tailored Privacy
- Privacy decision-making

Clemson
- Self-Actualization (NSF)
- Privacy decision-making for Training Systems (DoD) and IoT (Samsung + NSF)
Privacy is everywhere
BABY FIRST SALE
The one stop for all your baby’s firsts.

$18 set
Save $5
Baby bear overall and top set
New baby - 12 months.

20% off
Kids’ and babies’
clothing, underwear
and sleepwear
(new baby - 7)
See page 2 for exclusions.
Sorry, no price checks.

Also available in spot,
striped, ladybird and navy.

50% off
Hipod

$124
Save $60
The Hipod Mint
convertible car seat
Features high sides
wings for superior side impact protection
Converts from rear to forward facing
Suitable from birth - 1 year old.

$6
Save $3

33% off
Red/Pink print overall.
Cupcakes.
New baby - 18 months.
Snap off opening for easy dressing.

No deposit lay-by
on kids’ and babies’
clothing (new baby - 7)
and nursery until 30 January.
Not available on sale.

A huge range of kids’ and babies’
clothing (new baby - 7) and nursery
on sale for 2 weeks until Wednesday, 30 January 2013.
HEY!
YOU'RE
HAVING
A BABY!

How your shopping habits reveal even the most personal information. By Charles Dubigg
Motivation

How can we help users to balance the benefits and risks of information disclosure in a user-friendly manner, so that they can make good privacy decisions?
Outline

Show that technical solutions do not work

Show that transparency and control do not work

Show that privacy nudges are also lacking

Argue that privacy decision support needs to be personalized

Investigate personalization parameters

Demonstrate the potential effects on user experience
Why user-tailored privacy?

Problems with transparency and control, and with privacy nudges.
Technical solutions

As engineers, we would first go for a technical solution

- Homomorphic encryption
- Differential privacy
- Data obfuscation
- Client-side personalization

Problem: How to convince users that this is better?
Client-side personalization

Let’s say you want to use users’ data for personalization in a mobile app recommender…

…which type of situation are users most comfortable with?

- “Your data will be sent to, and analyzed by a company called American Personalization.”
- “All personalization happens client-side.”
- “Your data will be sent to, and analyzed by Amazon.”
- “Your data will be sent to, and analyzed in the cloud.”
Client-side personalization

Perceived Privacy Protection

System-specific Privacy Concerns

Kobsa et al., JASIST 2016
Client-side personalization works, but only for people with **high overall privacy concerns**

Client-side personalization brought up **other issues**:  

“What happens if my phone gets stolen?”  

“Can I lock my user model remotely so the thief can’t get to it?”  

“Is there a backup of my user model?”

Kobsa et al., CHI 2014
A human issue

The concept of privacy is an inherently human attitude

People make assumptions and form opinions about the collection, distribution and use of disclosed data.

Disclosure itself is a human behavior

In the end, people decide whether they want to disclose or not.

Regardless of our technical solutions, we should help them with that decision.
Transparency and control

Privacy Calculus: People weigh the risks and benefits of disclosure

Prerequisites of the privacy calculus are:

- being able to control the decision;
- having adequate information about the decision.

Transparency and control empower users to regulate their privacy at the desired level.
Why this doesn’t work

Transparency paradox:

Simple privacy notices aren’t useful, but detailed notices are too complex.

(Nissenbaum 2011)

Control paradox:

Consumers claim to want full control over their data, but they eschew the hassle of actually exploiting this control!

(Compañò and Lusoli 2010; Knijnenburg et al. 2013)
Fixing transparency

Is this detailed enough?

“Review and control certain types of information tied to your Google Account by using Google Dashboard.”
Fixing transparency

Would you read this?

“Let’s say you would like to review and control all the things that are tied to your Google Account. You might want to remove an old device. Or unlink an application you don’t use anymore. On the Google Dashboard page you can view and change the settings of devices and applications tied to your account. You can also see other synchronized information, such as your Google Chrome browser bookmarks, your contacts, as well as the number of conversations you’ve had through gmail. On this dashboard you can manage these things (and more), change their settings, or remove them from your account.”
How about now?

Let's say you would like to review and control all things that are tied to your Google account.

I... I'm not sure who is saying that... but yes, I would like to review and control all things that are tied to you— I mean, my Google account.

You might want to remove an old device...

I can finally remove my old phone now!!

My new Samsung Galaxy Note 7 is explosively better!!

Or unlink an old app... a very old app...

Oh no... th... this can't be real...

That the world has forgotten... no one uses MySpace anymore!!!!
OR UNLINK AN OLD APP... A VERY OLD APP...

THAT THE WORLD HAS FORGOTTEN...

NO ONE USES MYSPACE ANYMORE!!!!

1,000+ CONTACTS?! I DON'T EVEN KNOW HALF OF THESE PEOPLE!

IT ALSO SHOWS THE NUMBER OF CONVERSATIONS YOU'VE HAD THROUGH EMAIL.

LET'S GET RID OF ALL OF THE APPS I DON'T USE ANYMORE.

WELL, I DID HAVE GMAIL FOR A WHILE NOW...
Comics for privacy

Currently running a study testing comics vs. text at various levels of detail

Hypothesis: Comics can make privacy notices inviting, engaging, comprehensible, and memorable

Extra advantage for people with dyslexia or low literacy (target user group for a future study)

Knijnenburg and Cherry, SOUPS 2016
Fixing control

Modern browsers offer an auto-completion feature that reduces the effort of filling out web forms. These tools may cause users to complete more fields than they intended. They make it so easy to submit a fully completed form that users may skip weighing benefits and risk.
Create a Profile

Please create your profile by entering your information below. Note that FormFiller will store the information locally on your device, and only for the duration of this study. We will never submit any forms automatically or disclose this information to others without your active involvement.

About you:

First name: 

Last name: 

Gender: 

Age: 

Address: 

City: 

State: 

Zip: 

E-mail: 

Phone: 

Tastes and Preferences:

Favorite movie: 

Favorite band/artist: 

Favorite food: 

Favorite weekend pastime: 

Last holiday location: 

Political views: 

Work and education:

Current/previous job: 

Sector: 

Employment status: 

Work experience (yrs): 

Income level: 

Highest completed degree: 

Computer skills: 

Health and lifestyle:

Overall health: 

Dietary restrictions: 

Number of doctor visits last month: 

Weight (lbs): 

Birth control usage (you or your partner): 

Medical conditions:

- Diabetes
- Hypertension
- Respiratory (COPD etc.)
- High cholesterol
- Overweight
- Heart problems / chest pain
- Obesity
- Digestive problems
- Seasonal allergies
- Back / neck problems
- Frequent headaches
- Arthritis / rheumatism
- Cancer

None that are mentioned
About you:

First name: ____________________________  Last name: ____________________________

Gender: ________________________________

Age: ________________________________

Address: ______________________________

City: ________________________________  State: ________________________________  Zip: ________________________________

E-mail: ________________________________

Phone: ________________________________

Tastes and Preferences:

Favorite movie: ________________________________

Favorite band/artist: ________________________________

Favorite food: ________________________________

Favorite weekend pastime: ________________________________

Last holiday location: ________________________________

Political views: ________________________________
Study Procedures

543 Amazon Mechanical Turk participants first entered a wide range of info into an auto-completion tool:

Create a Profile

Please create your profile by entering your information below.

Note that FormFiller will store the information locally on your device, and only for the duration of this study. We will never submit any forms automatically or disclose this information to others without your active involvement.

About you:

First name: 
Last name: 
Gender: 
Age: 
Address: 
City: 
State: 
Zip: 
E-mail: 
Phone:

Tastes and Preferences:

Favorite movie: 
Favorite band/artist: 
Favorite food: 
Favorite weekend pastime: 
Last holiday location: 
Political views:

Work and education:

Current/previous job: 
Sector: 
Employment status: 
Work experience (yrs): 
Income level: 
Highest completed degree: 
Computer skills

Health and lifestyle:

Overall health: 
Dietary restrictions: 
Number of doctor visits last month: 
Weight (lbs): 
Birth control usage (you or your partner): 
Medical conditions:

- Diabetes
- Respiratory (COPD etc.)
- Overweight
- Hypertension
- High cholesterol
- Heart problems / chest pain
- None that are mentioned
Create a Profile

Please create your profile by entering your information below. Note that FormFiller will store the information locally on your device, and only for the duration of this study. We will never submit any forms automatically or disclose this information to others without your active involvement.

**About you:**
- First name: 
- Last name: 
- Gender: 
- Age: 
- Address: 
- City: 
- State: 
- Zip: 
- E-mail: 
- Phone: 

**Tastes and Preferences:**
- Favorite movie: 
- Favorite band/artist: 
- Favorite food: 
- Favorite weekend pastime: 
- Last holiday location: 

**Health:**
- Medical conditions: 
- Dietary restrictions: 
- Income level: 
- Weight (lbs): 
- Employment status: 
- Experience (years): 
- Current/previous job: 
- Education: 
- Highest completed degree: 
- Political views: 
- Overall health: 
- Birth control usage: 
- Respiratory (COPD etc.): 
- Diabetes: 
- Obesity: 
- Heart problems / chest pain: 
- Hypertension: 
- Digestive problems: 
- Back / neck problems: 
- Arthritis / rheumatism: 
- High cholesterol: 

**Employment:**
- Work and education: 
- How did you hear about this study? (part 1/3)

**BlogHeroes**

Some guilds write about their health. Providing us with some info will help us match them to you.

**For employers**

Some guilds write about their jobs. Tell us more about yours, and we can provide a better match.

**Contact**

Please provide some background info to get our matching process started.

**About us**

Your personal Codacare health insurance policy will be based on the information you provide. Please note that none of the items are required, but the insurance will be better tailored to your needs if you provide more information.
Study Procedures

Each site corresponds to a particular type of info:

- blogging community = personal interest items
- job search website = job skills items
- health insurer = health record items

They requested all the info, not just the relevant stuff!
Research outline

We introduce **two new efficacy-increasing designs**

We compare three tools:

- **Auto FormFiller**: auto-fills fields, users can remove manually
- **Remove FormFiller**: click to remove each field
- **Add FormFiller**: click to fill each field
Fixing control

Disclosure was **not purpose-specific** for users of the Auto FormFiller.

Disclosure was **purpose-specific** for users of the Remove and Add FormFillers.

Knijnenburg et al., ICIS 2013
Privacy decisions are too hard!

Most systems are much too complex

- Privacy policies are increasing in length; Milne et al. 2006
- Facebook’s privacy controls are “Labyrinthian”; Consumer Reports 2012

Conclusion: Transparency and control do not work!

- “a red herring”; Barocas and Nissenbaum 2009
- “paradigm has failed”; Nissenbaum 2011
- “fail to provide people with meaningful control”; Solove 2013
Alternative: privacy nudges

Subtle yet persuasive cues that makes people more likely to decide in one direction or the other.

(Thaler and Sunstein 2008)

Examples of nudges:

– **Justification**: a succinct reason to disclose or not disclose a certain piece of information.

– **Default**: make the best action the easiest to perform.
Why this doesn’t work

What is the “right” direction of a nudge?

- **More disclosure**: better personalization, but some may feel tricked.

- **More private**: less threat, but harder to enjoy the benefits of disclosure.

- Going for the **average** (e.g. “smart default”, Smith et al. 2013): impossible, because people vary too much.

**Solution**: move beyond the one-size-fits-all approach!
Towards a user-tailored approach to privacy

Exploring the potential for personalization.
Beyond one-size-fits-all

Idea: Give people privacy recommendations!

“Figure out what people want, then help them do that.”

Step 1: Find determinants of privacy calculus.

These can become the “personalization parameters”.

Step 2: Adapt the nudge to the context.

Test how this would influence the user experience.
# Information ("what")

<table>
<thead>
<tr>
<th>Type of data</th>
<th>ID</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook activity</td>
<td>1</td>
<td>Wall</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Status updates</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Notes</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Shared links</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Photos</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td>Hometown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Location (city)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Location (state/province)</td>
</tr>
<tr>
<td>Contact info</td>
<td></td>
<td>Residence (street address)</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Phone number</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Email address</td>
</tr>
<tr>
<td>Life/interests</td>
<td>13</td>
<td>Religious views</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Interests (favorite movies, etc.)</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Facebook groups</td>
</tr>
</tbody>
</table>

"What?" = Four dimensions
159 pps tend to share little information overall (LowD)
26 pps tend to share activities and interests (Act+IntD)
50 pps tend to share location and interests (Loc+IntD)
65 pps tend to share everything but contact info (Hi-ConD)
59 pps tend to share everything

Knijnenburg et al., IJHCS 2013
Privacy profiles

Winsniewski, Knijnenburg, and Lipford, IJHCS 2017
see www.usabart.nl/chart
Adapt the interface

More prominent audience selection (selective sharers)

More prominent timeline moderation (time savers)

Wilkinson et al., USEC 2017
Adapt the order

Attribute weights $w_a$

7 Attributes $\alpha$

Recommendations $i$

Rank by $U_i$, limit to top $N$

Attribute values $v_{i,a}$

MAUT: $U_i = \sum w_a \cdot v_{i,a}$

Software-Coaches.com

Energy Saving Coach$^{beta}$

Choose measures?

Indicate preference?

Show totals in $\text{US}\$ kWh

You are your recommendations; select the measures you want to do

Move your mouse over these attributes to learn more about them

Attribute weights $w_a$

7 Attributes $\alpha$

Recommendations $i$

Rank by $U_i$, limit to top $N$

Attribute values $v_{i,a}$

MAUT: $U_i = \sum w_a \cdot v_{i,a}$
Preference elicitation

The best preference elicitation method (PE-method) depends on users’ domain knowledge.

E.g. energy-saving (Knijnenburg and Willemsen 2009, 2010; Knijnenburg et al. 2011, 2014).

Our studies show:

- Energy-saving experts prefer systems that allow direct control over attribute weights.
- This doesn’t work well for novices.
New: demographics-based PE
New: demographics-based PE

Demographics are an important determinant of preferences in the domains of energy and health.

- Needed: an algorithm that translates answers to demographic questions into attribute weights.
- Based on these weights I can then recommend items as usual.

Demographics-based PE:
- May be most beneficial for domain novices (known and easy to report).
- May be more privacy-sensitive than other PE-methods (Ackerman et al. 1999).

“Privacy-personalization paradox”
Adaptive request order

Which item to ask first?

Not all items are equally useful to the recommender.
Not all demographic items are equally sensitive.
Not everyone is equally private regarding their demographics.

Knijnenburg, dissertation 2015
Adaptive request order

\[ u_o = \sum_{r_{oa}} \frac{v_r}{d_{an}} \]

where

\[ d_{an} = \text{abs}(w_{an} - \bar{w}_n) + .0001 \]

\[ r_i = \begin{cases} 
  u_i & \text{if } \delta_i < \alpha, \\
  -\delta_i & \text{if } \delta_i > \alpha.
\end{cases} \]

\[ p_{ni} = \frac{e^{\beta_{n} - \delta_i}}{1 + e^{\beta_{n} - \delta_i}} \]

Usefulness

Sensitivity

Trade-off

Tendency

\[ \beta_n = \text{mean}_n(\delta) + \sqrt{1 + \text{var}_n(\delta)}/2.9 * \ln\left(\frac{|D_n|}{|L_n| - |D_n|}\right) \]

and \[ \alpha_n^H = \beta_n - 1.5 \]
Outcome

The adaptive request order did not result in the hypothesized benefits.

However, other (static) versions that automatically traded off usefulness and sensitivity did improve users’ experience.

Reserved optimism: Automatic means to relieve some of the burden of controlling one’s privacy settings are still promising.

Future work may further improve the truly adaptive versions.

Goal: a universal method that works for all kinds of users.
General conclusion

Summary and discussion of societal impact
My contribution

I argued that privacy scholars need to move beyond the “one-size-fits-all” approach to privacy.

In several studies, I contextualized users’ privacy decisions.

I presented the idea of “user-tailored privacy.”
Societal impact

User-tailored privacy:

Relieves some of the burden of controlling privacy, while at the same time respecting each individual’s preferences.

Provides **realistic empowerment**: the right amount of transparency and the right amount of control.

Refrains from making moral judgments about what the “right” level of privacy should be.

The best way forward to support people’s privacy decisions!
Mentioned papers

• Kobsa et al., CHI 2014: Let’s Do It at My Place Instead? Attitudinal and Behavioral Study of Privacy in Client-Side Personalization

• Kobsa et al., JASIST 2016: The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach

• Knijnenburg and Cherry, SOUPS 2016: Comics as a Medium for Privacy Notices.

• Knijnenburg et al., ICIS 2013: Counteracting the Negative Effect of Form Auto-completion on the Privacy Calculus.

• Knijnenburg et al., IJHCS 2013: Dimensionality of information disclosure behavior

• Wisniewski et al., IJHCS 2017: Making privacy personal: Characterizing social network users by their privacy proficiency and management strategies.

• Wilkinson et al., USEC 2017: User-Tailored Privacy by Design.

• Knijnenburg, dissertation 2015: A user-tailored approach to privacy decision support.