Usable Privacy Technologies

Bart P. Knijnenburg
@usabart

Find me at:
www.usabart.nl + bartk@clemson.edu

Hello, I'm Bart

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

Clemson University (Assoc. Prof.)

UC Irvine (PhD)

Carnegie Mellon University (M)

TU Eindhoven (BS + MS)

My son Tolga (who wants to be a farmer when he grows up)

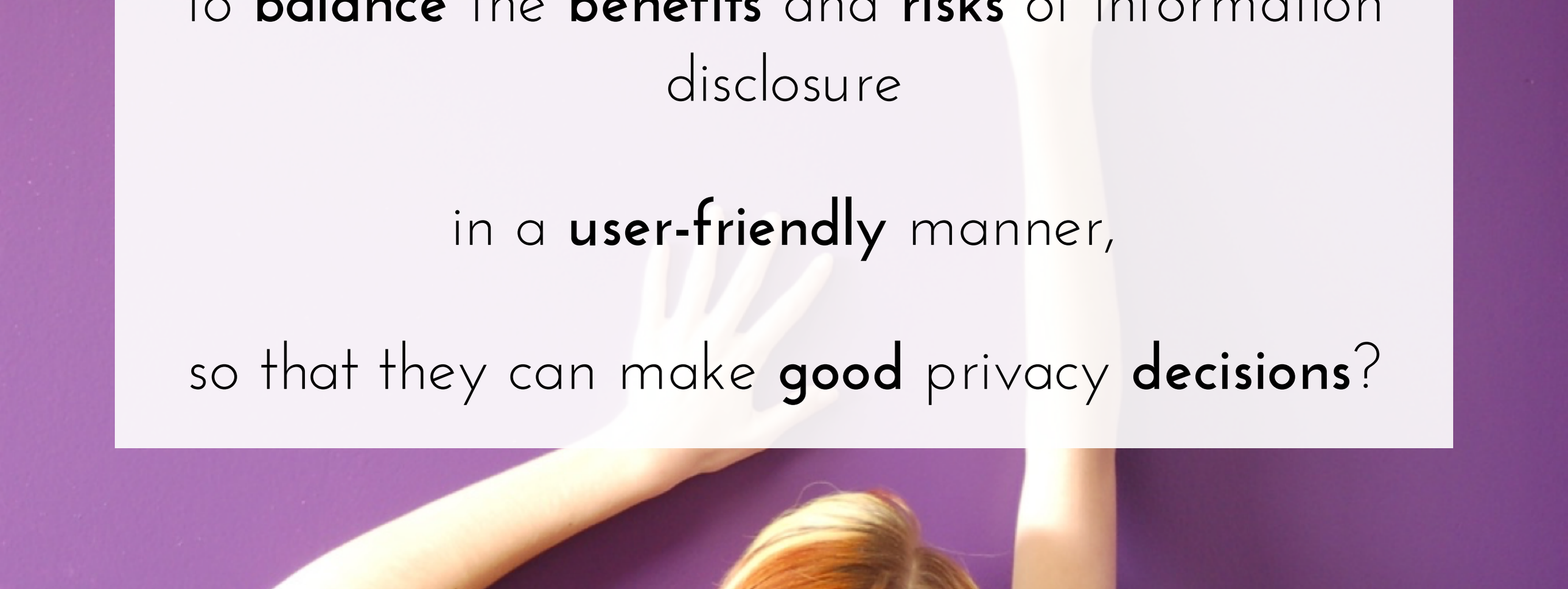
Privacy

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 existing solutions to make privacy technologies more usable do not work

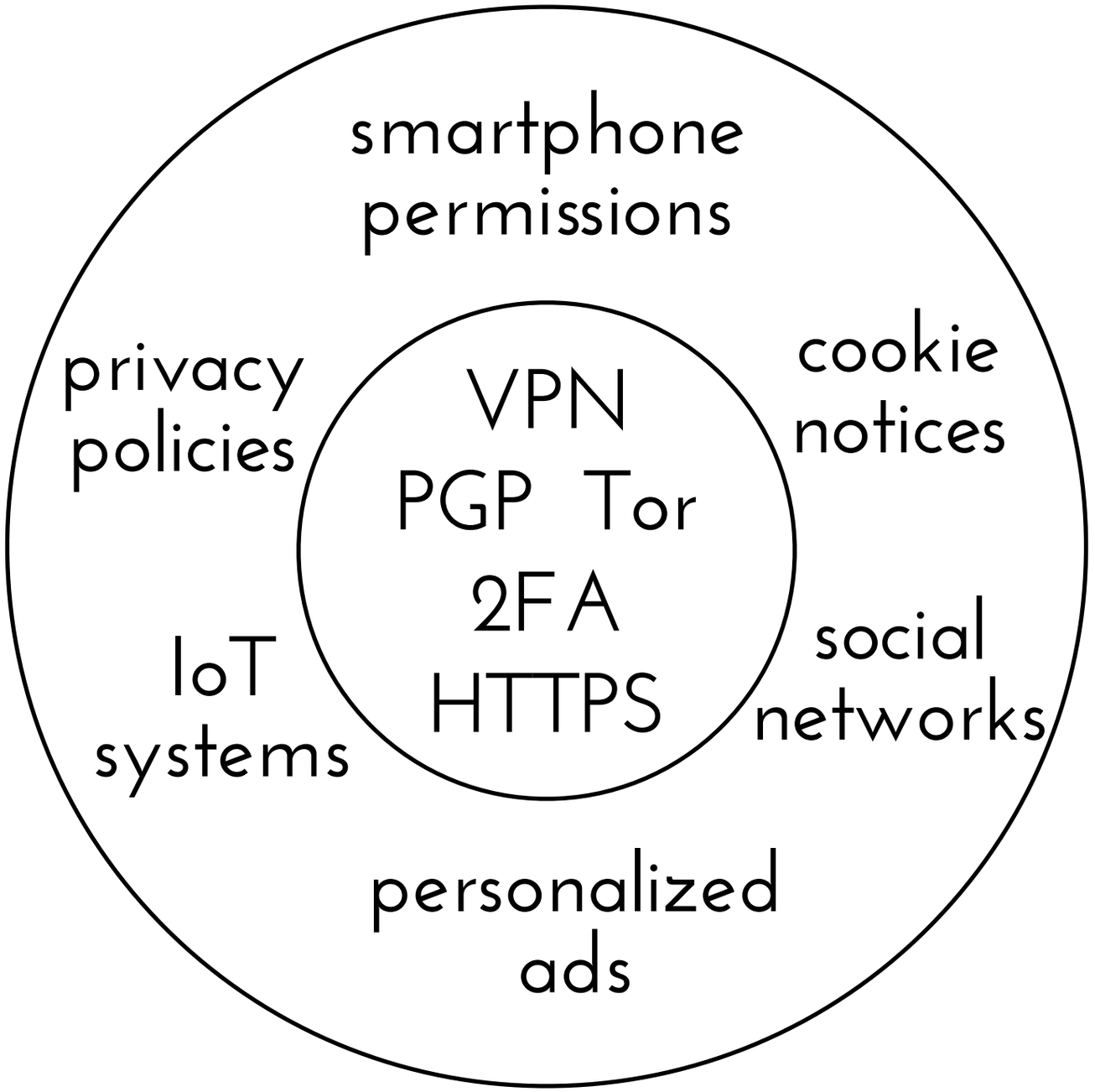
Argue that we must either design for elaboration…

…and/or design personalized privacy decision support

Usable Privacy Technologies

A tale of transparency and control

What are privacy technologies?



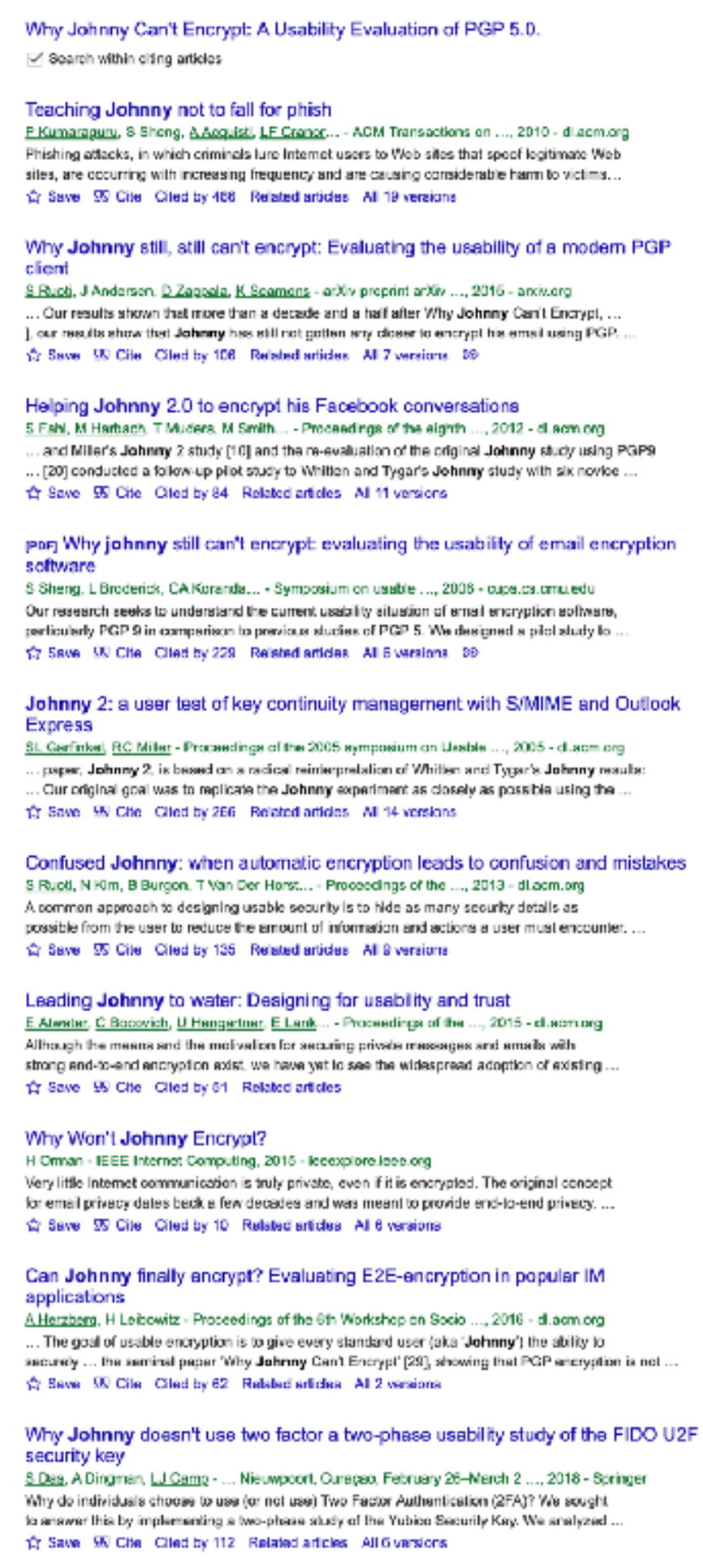
Seasons (2022) "Privacy-Enhancing Technologies"

Making privacy

Early work: Why are privacy technologies not usable?

Whitten & Tygar (1996) "Why Johnny Can't Encrypt – A Usability Evaluation of PGP 5.0"

A slew of "Johnny papers" followed



Making privacy usable?

Nowadays: several conferences / tracks that cover usable privacy

Symposium On Usable Privacy and Security (SOUPS)

Privacy Enhancing Technologies Symposium (PETS)

Privacy track at the ACM conference on Human Factors in Computing Systems (CHI) and the ACM conference on Computer-Supported Collaborative Work and Social Computing (CSCW)

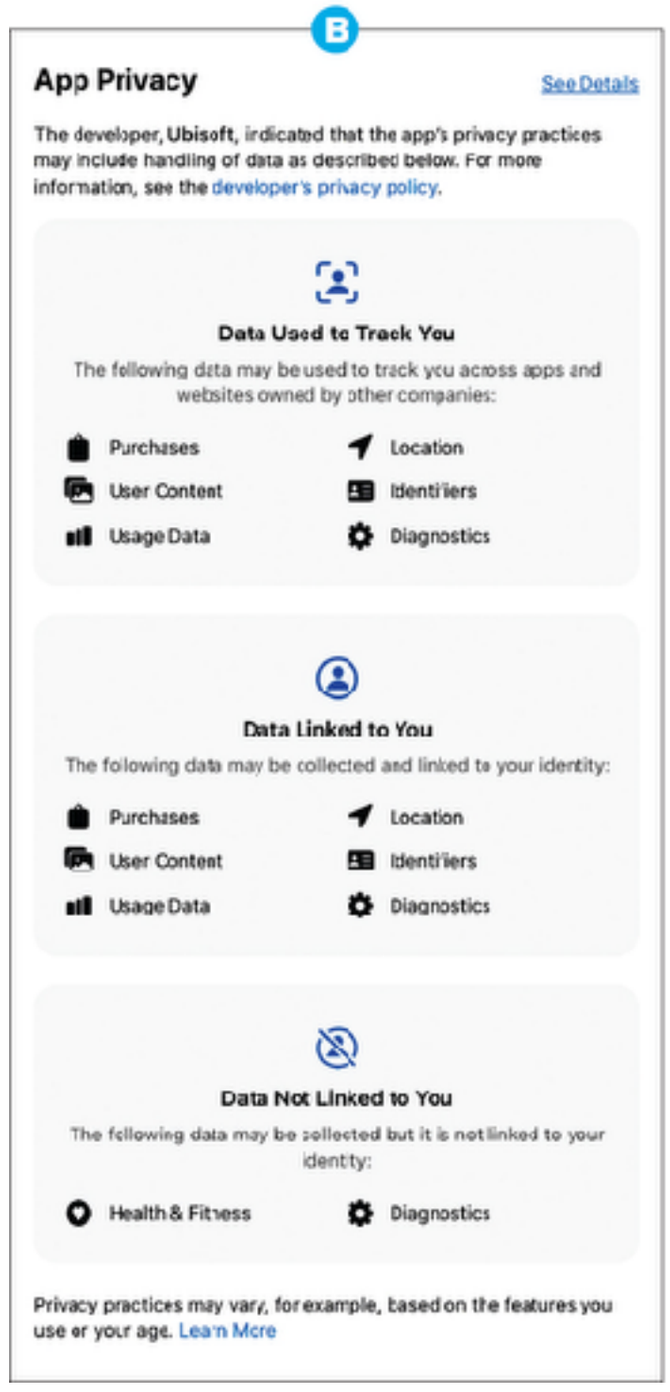
Ex 1: privacy nutrition labels

Early academic work:

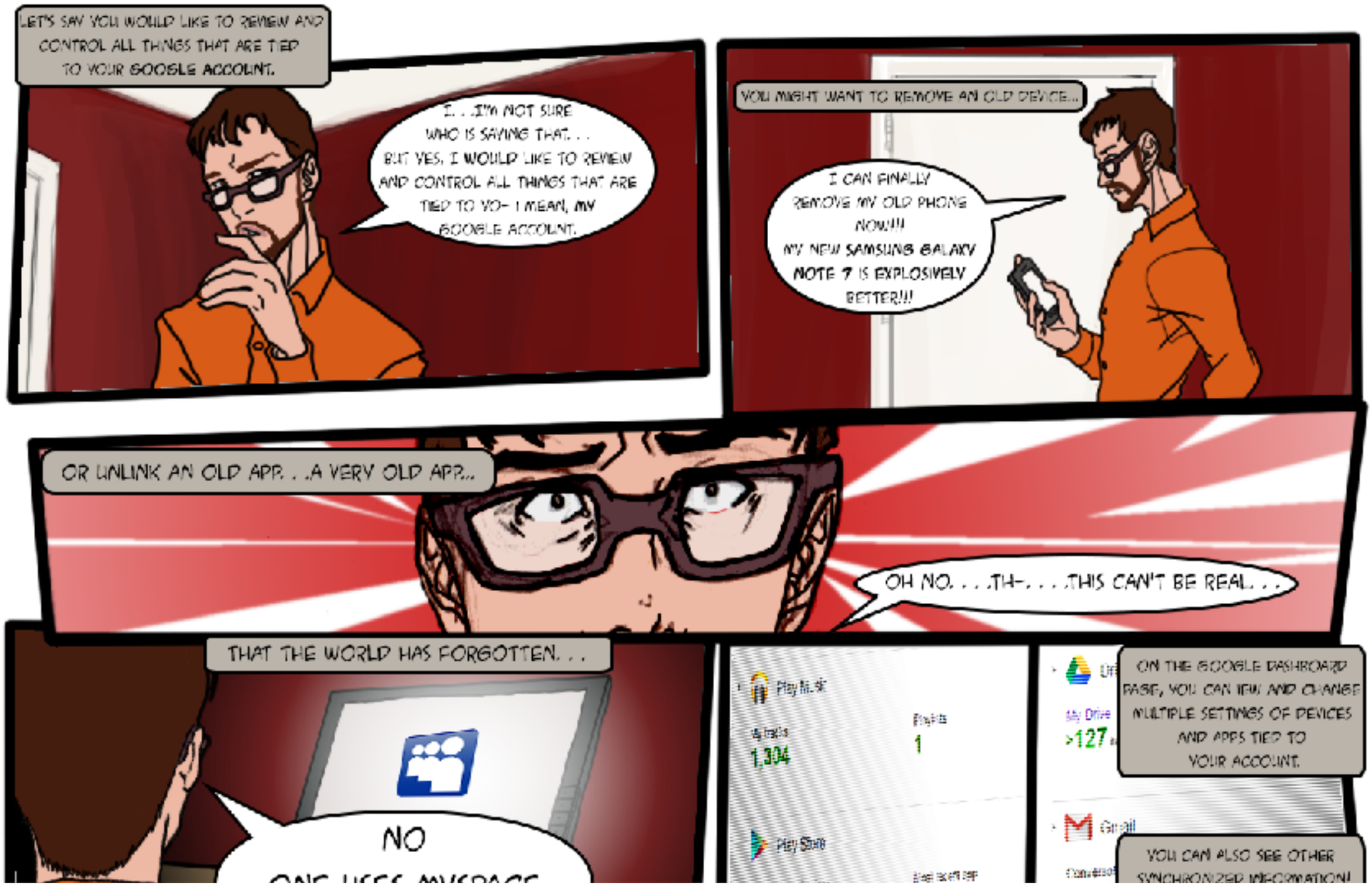
> Kelly et al. (2009) "A "Nutrition Label" for Privacy"

Implementation in iOS and Android in 2020 rather disappointing:

> Cranor (2022) "Mobile-App Privacy Nutrition Labels Missing Key Ingredients for Success"



Ex. 2: privacy policy comics



Knijnenburg and Cherry (2016) "Comics as a Medium for Privacy Notices"

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!!!!

Play Music
My tracks
1,304
Playlists
1

Play Store
Apps you've installed
232

Drive
My Drive
>127

Gmail
Conversations
443

ON THE GOOGLE DASHBOARD PAGE, YOU CAN VIEW AND CHANGE MULTIPLE SETTINGS OF DEVICES AND APPS TIED TO YOUR ACCOUNT.

YOU CAN ALSO SEE OTHER SYNCHRONIZED INFORMATION!

SUCH AS YOUR GOOGLE CHROME BROWSER BOOKMARKS. . .

Contacts
All contacts
1,497

. . .OR YOUR CONTACTS. . .

Contacts
All contacts
1,497

All contacts
1,497

Drive
My
>127

OH...

MY...

GOD...

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

NEITHER DO I.

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

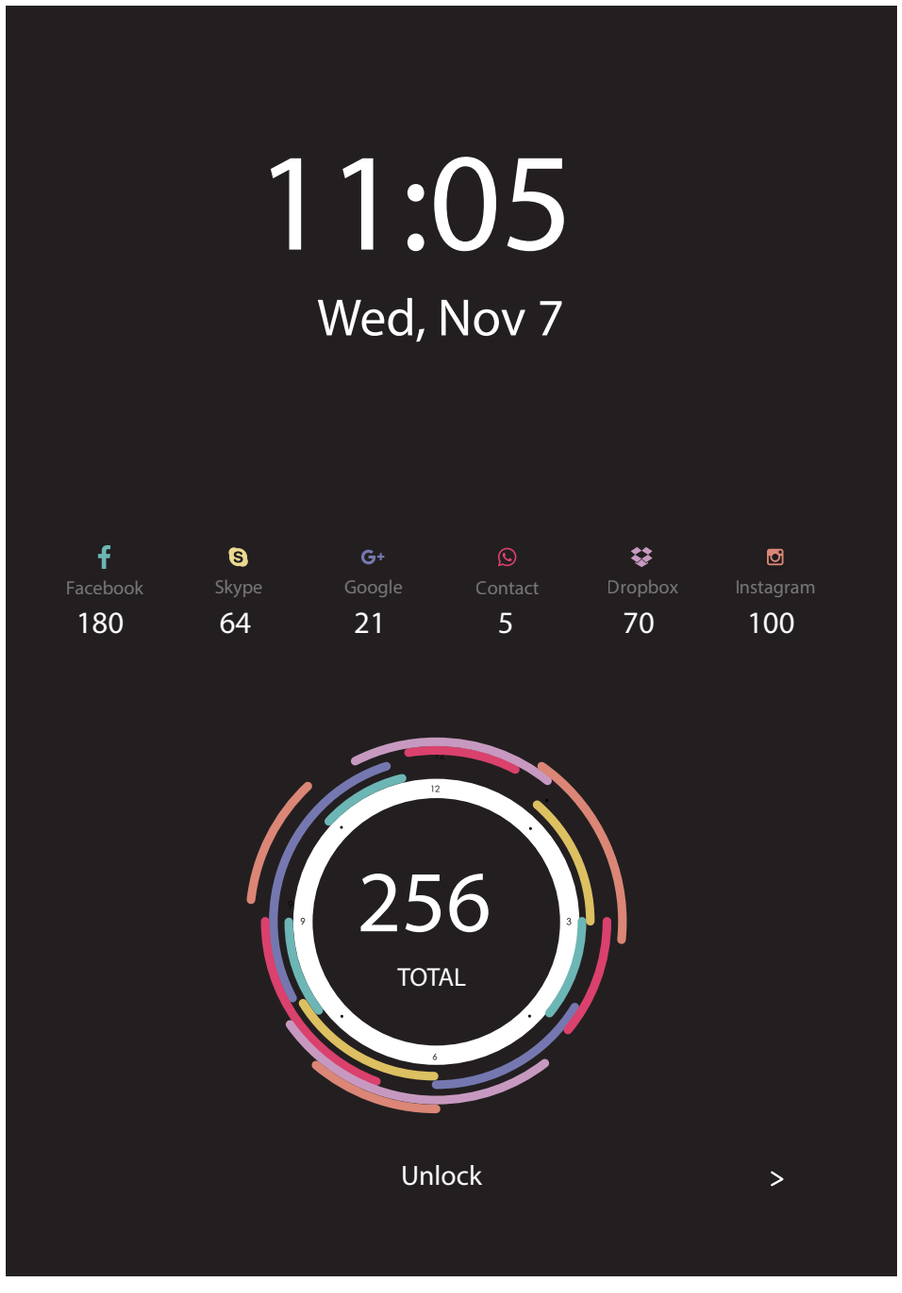
Gmail
Conversations
443

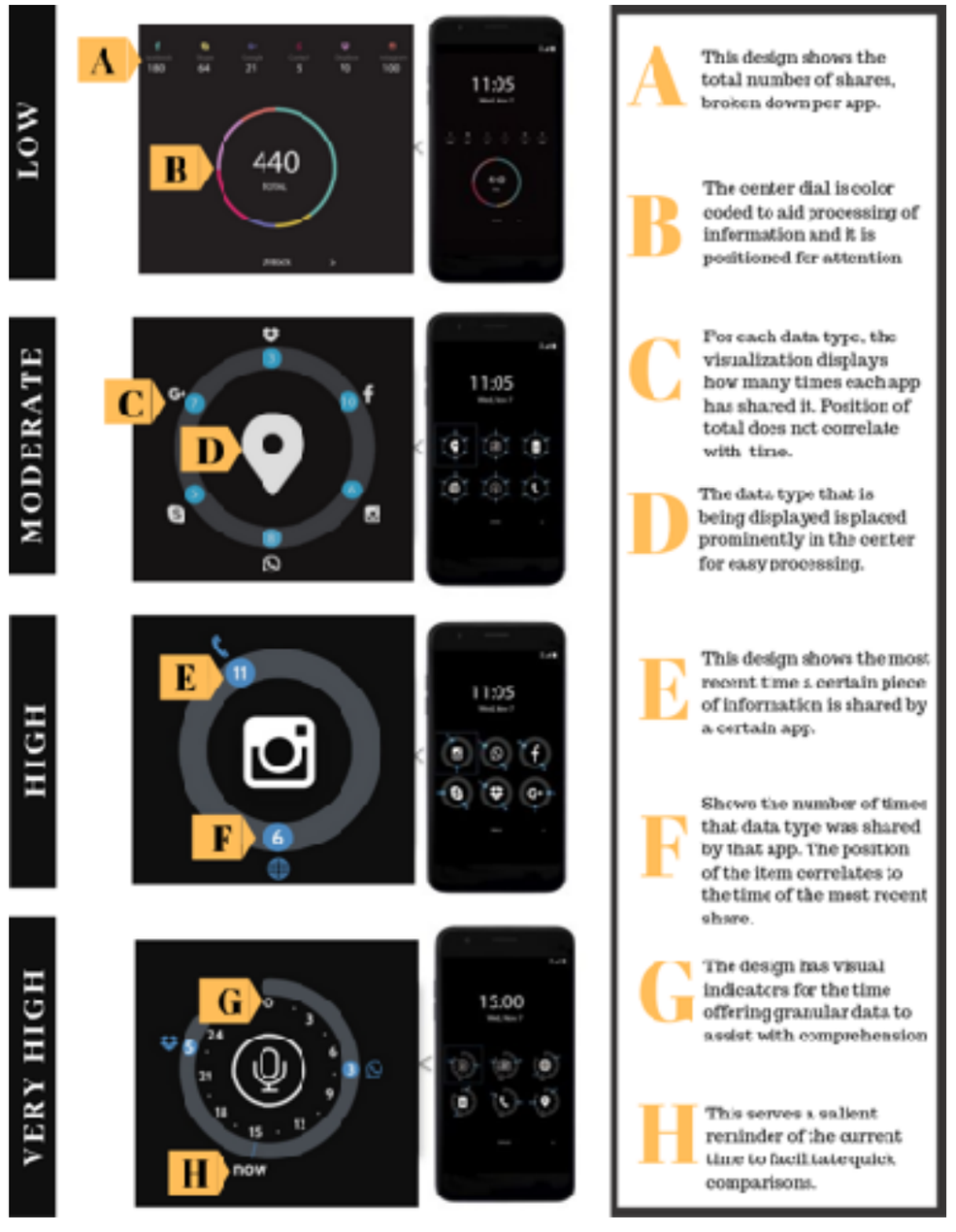
WELL, I *DID* HAVE GMAIL FOR A WHILE NOW. . .

ON THE DASHBOARD, YOU CAN MANAGE THESE THINGS (AND MORE), CHANGE THEIR SETTINGS OR REMOVE THEM FROM YOUR ACCOUNT!!

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

Privacy screensavers





Wilkinson et al. (2020) "Privacy at a Glance"

Ex 4: social circles

Most social networks allow you to define "circles" and share selectively

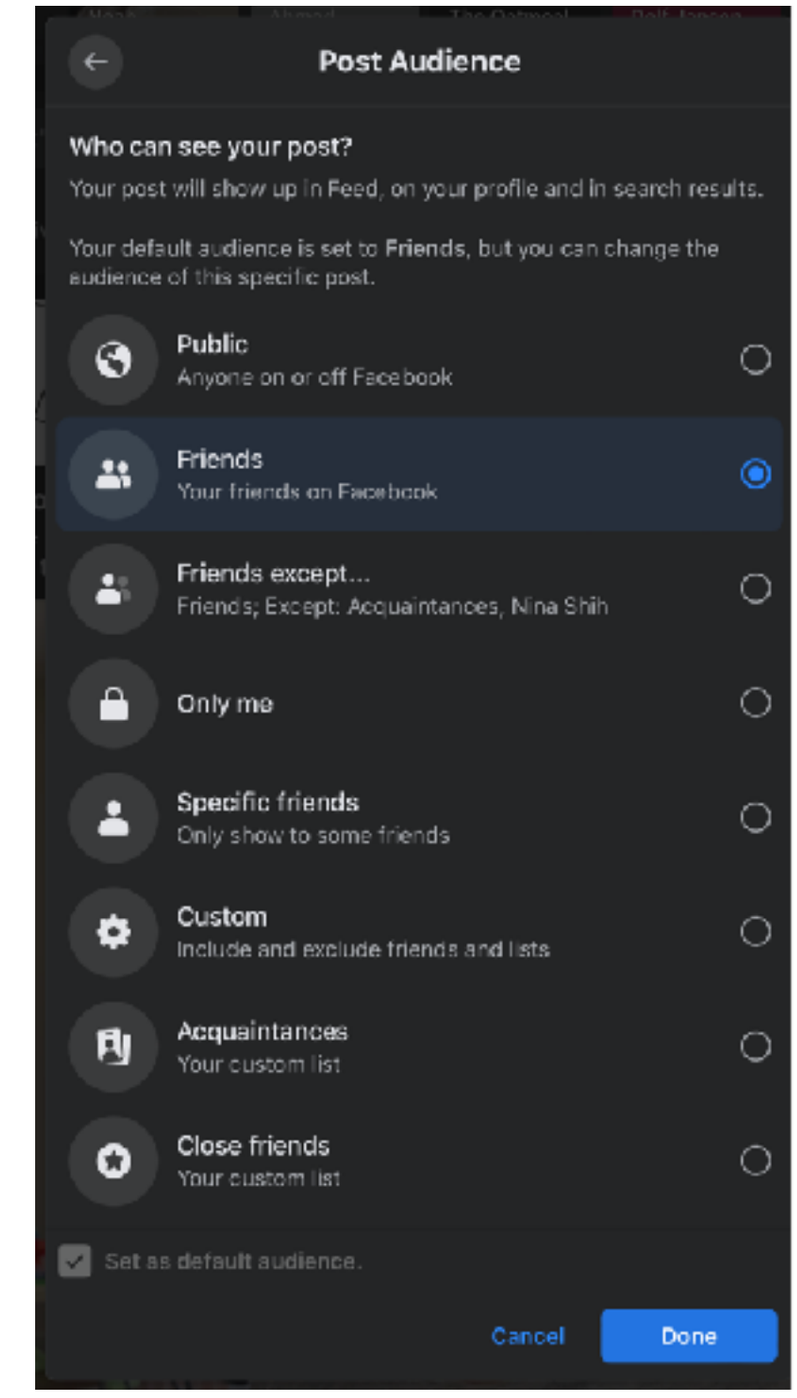
Most people don't do this

Strater & Lipford (2008) "Strategies and struggles with privacy in an online social networking community"

Watson et al. (2012) "+Your circles: sharing behavior on Google+"

Doesn't reduce threat of oversharing

Knijnenburg & Kobsa (2014) "Increasing Sharing Tendency Without Reducing Satisfaction"



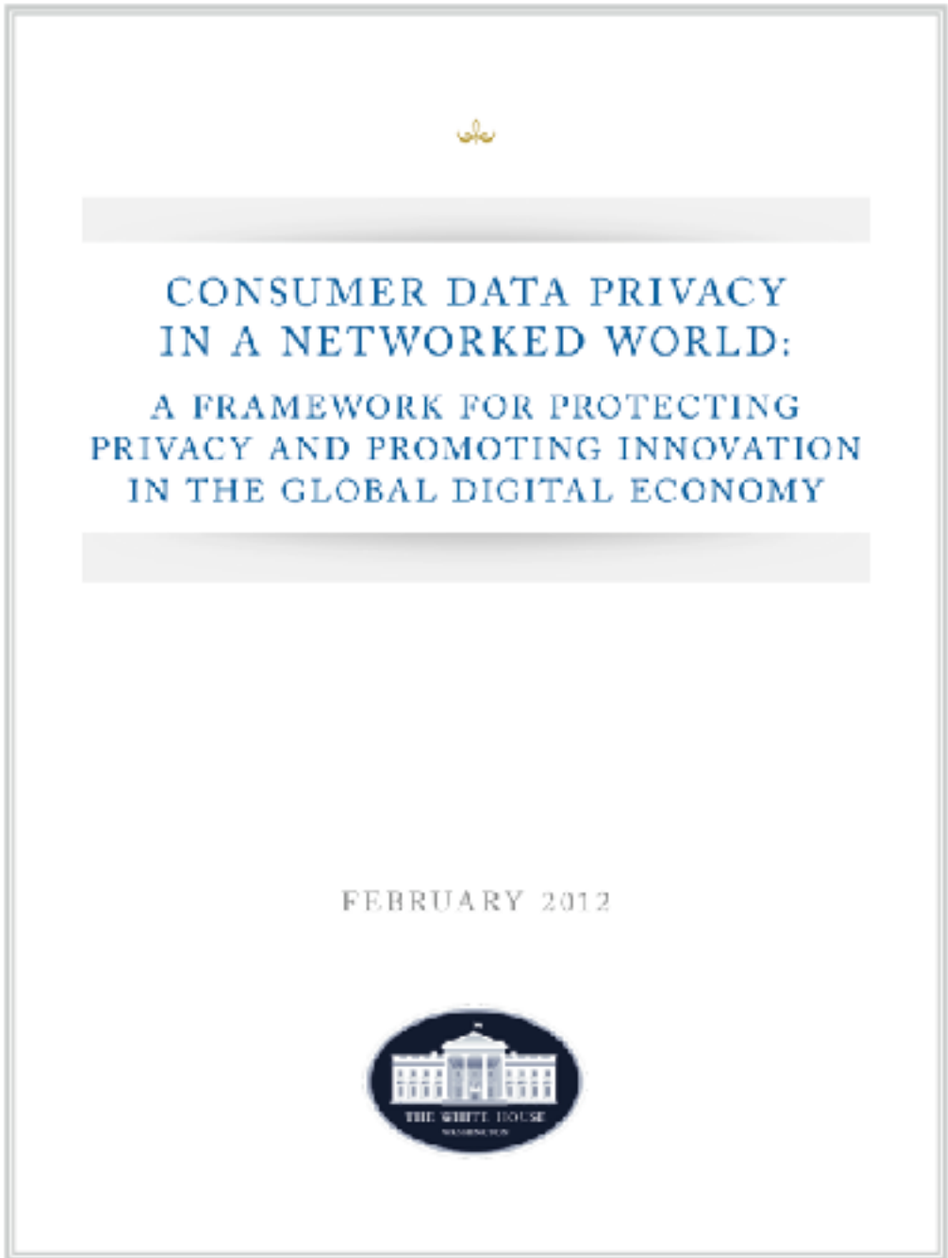
From the U.S. Privacy directive

Transparency (consent)

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

Control (empowerment)

"companies should offer consumers clear and simple choices [...] about personal data collection, use, and disclosure"



Death to the Privacy Calculus?

Why transparency and control don't actually work

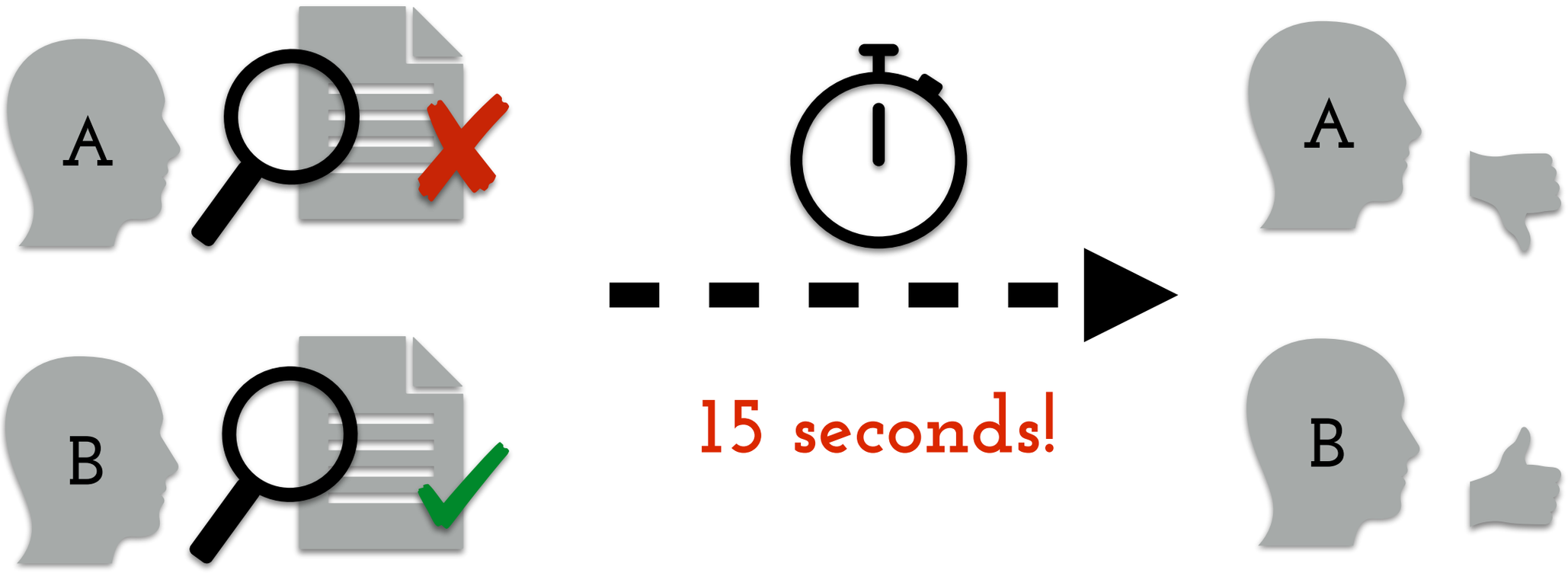
Transparency and control

Privacy Calculus: People weigh the risks and benefits of disclosure

Prerequisites of 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.



Quiz #1

After what length of time is the privacy policy no longer taken into account?

Quiz #2

Which version leads to more submitted forms?
With TRUSTe logo to without logo?

A	☐	Please send me Vortrex Newsletters and information.	25%
B	☐	Please do not send me Vortrex Newsletters and information.	37%
C	☒	Please send me Vortrex Newsletters and information.	53%
D	☒	Please do not send me Vortrex Newsletters and information.	0%

Figure 4: Subjects were assigned one of the following conditions in the registration page.

Quiz #3

Which version leads to more newsletter subscriptions?
Opt-in or opt-out? Negative or positive framing?

Why is this happening?

Transparency paradox (Nissenbaum, 2011):

> Privacy notices that are sufficiently detailed to have an impact are often too long for people to read

Control paradox (Compaño and Lusoli, 2010):

> While users claim to want full control over their data, they avoid the hassle of actually exploiting this control

Privacy Nudging

An alternative solution
(that also doesn't really work)

We can influence people!

Justification nudge

A succinct reason to disclose (or not disclose) information

Order nudge

Change request order to increase disclosure (foot-in-the-door, door-in-the-face)

Default/framing nudge

Set the default and/or framing in such a way that it increases or decreases disclosure

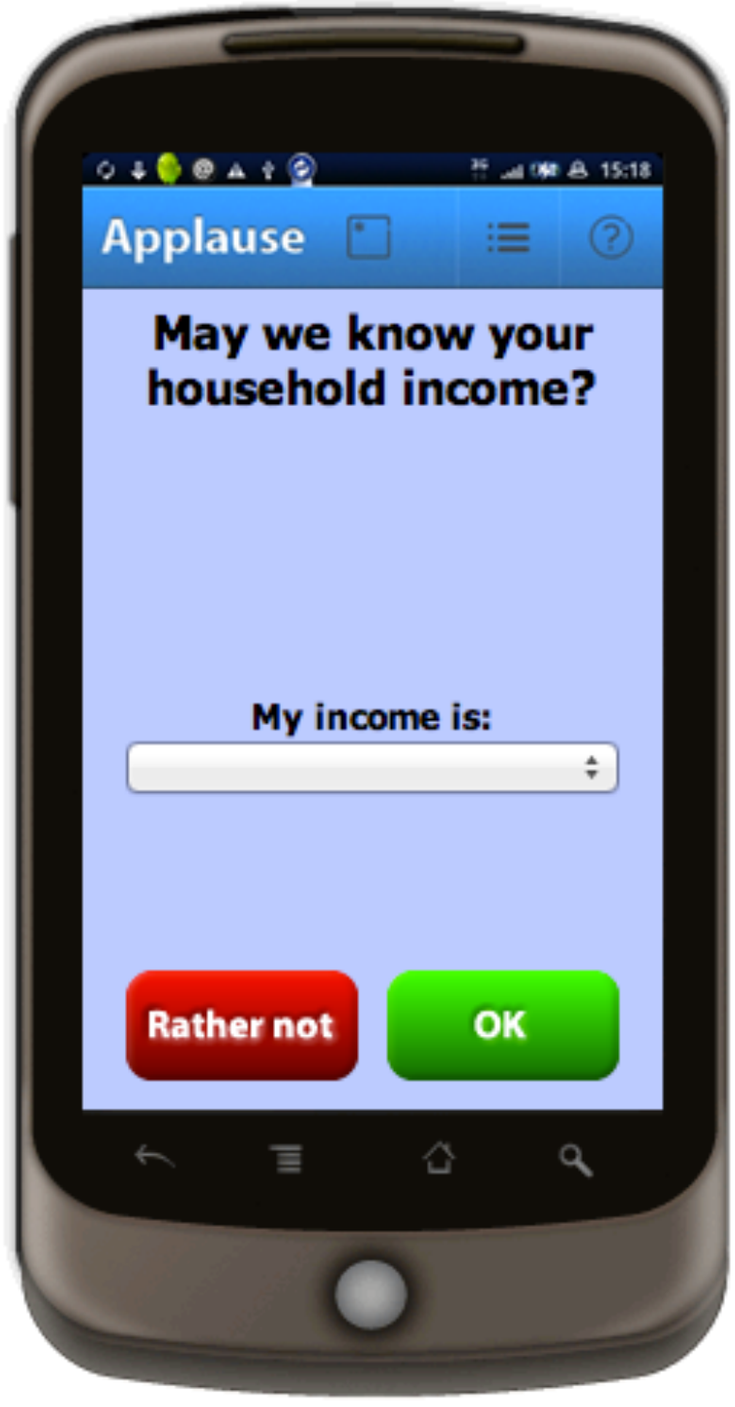
Nudge 1: justification

Mobile app recommender

Asks 31 questions
(12 context, 19
demographics)

Gives recommendations
based on users' answers

Users are allowed to
withhold information



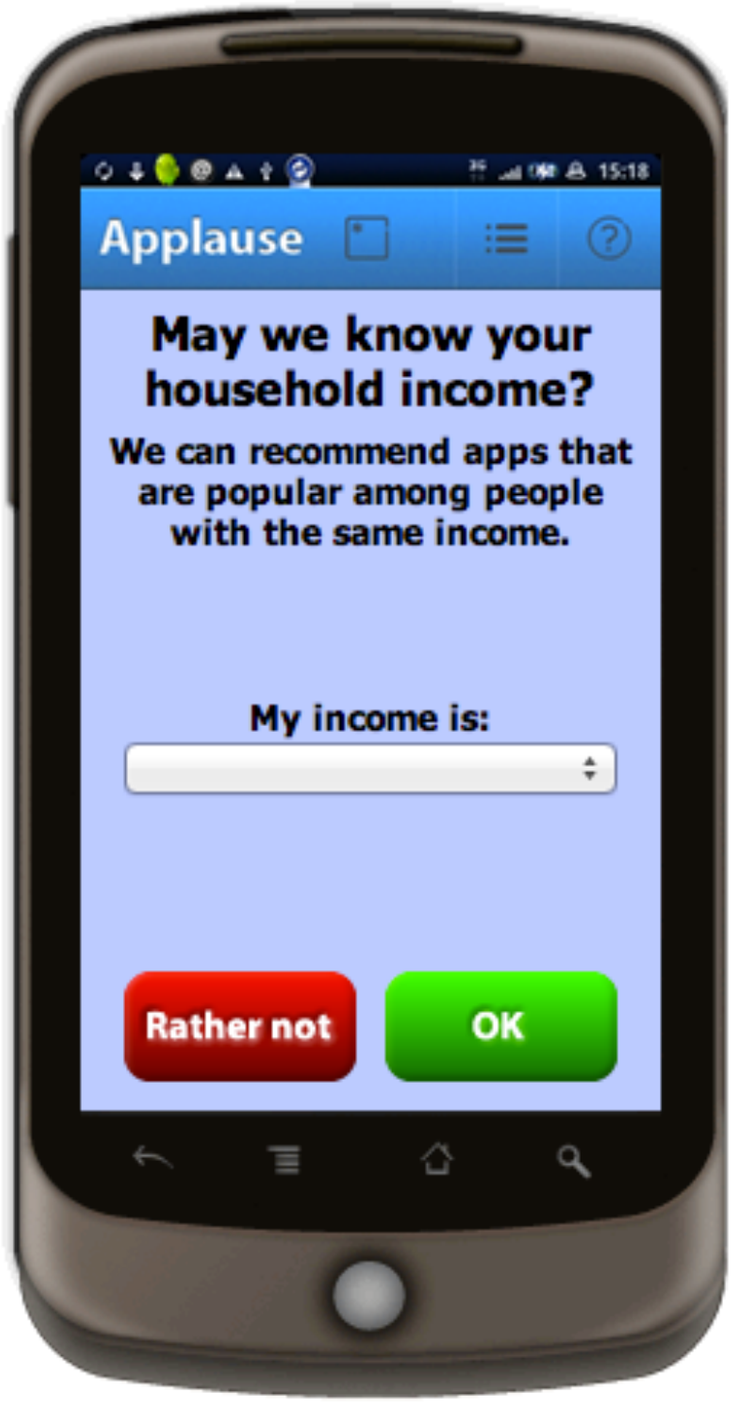
Nudge 1: justification

How useful is this for me?

How many others are disclosing this?

How useful was it for them?

What are you gonna do with it?



Nudge 2: Request order

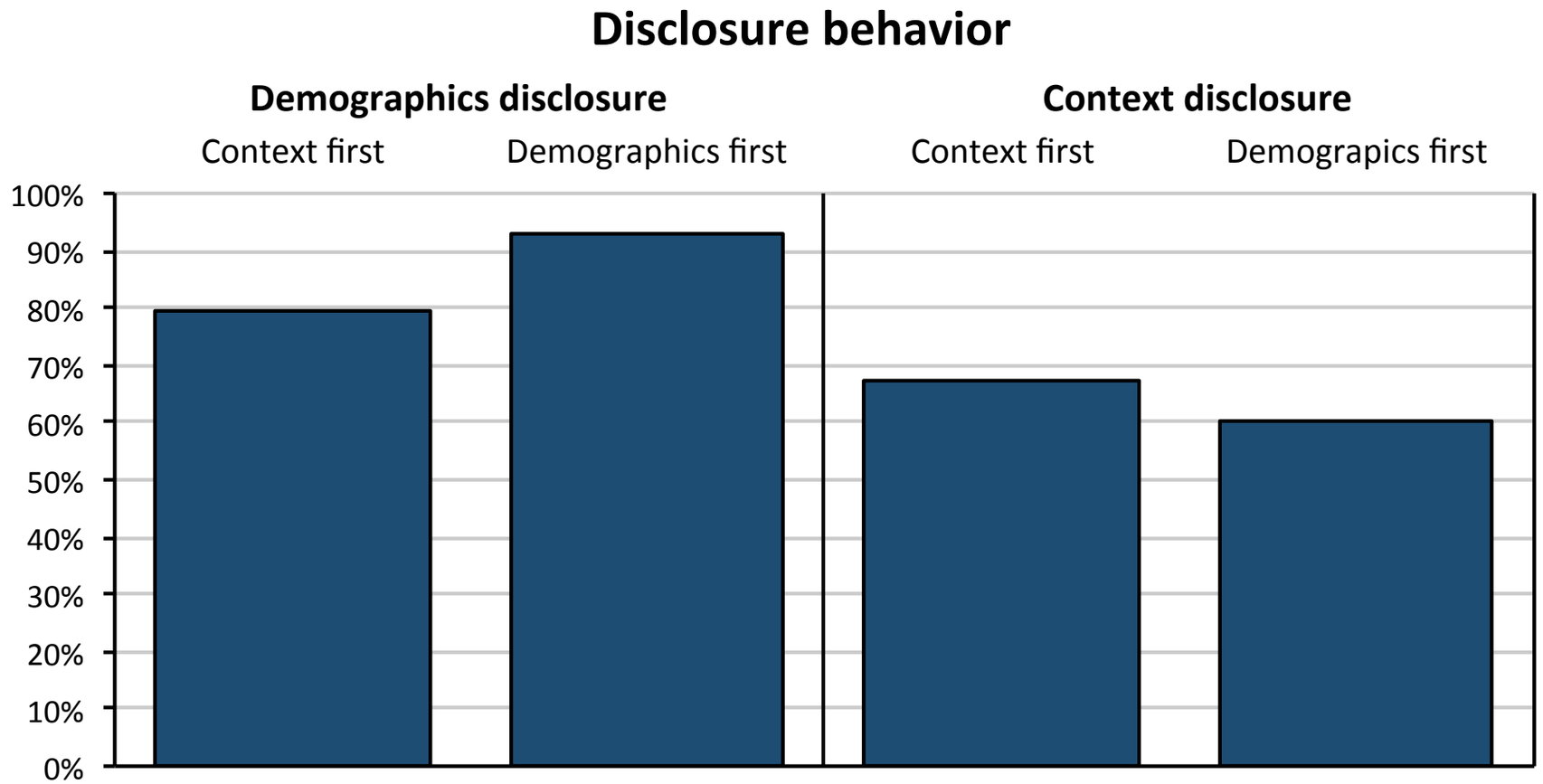
LOCATION, ETC.

GENDER, ETC.

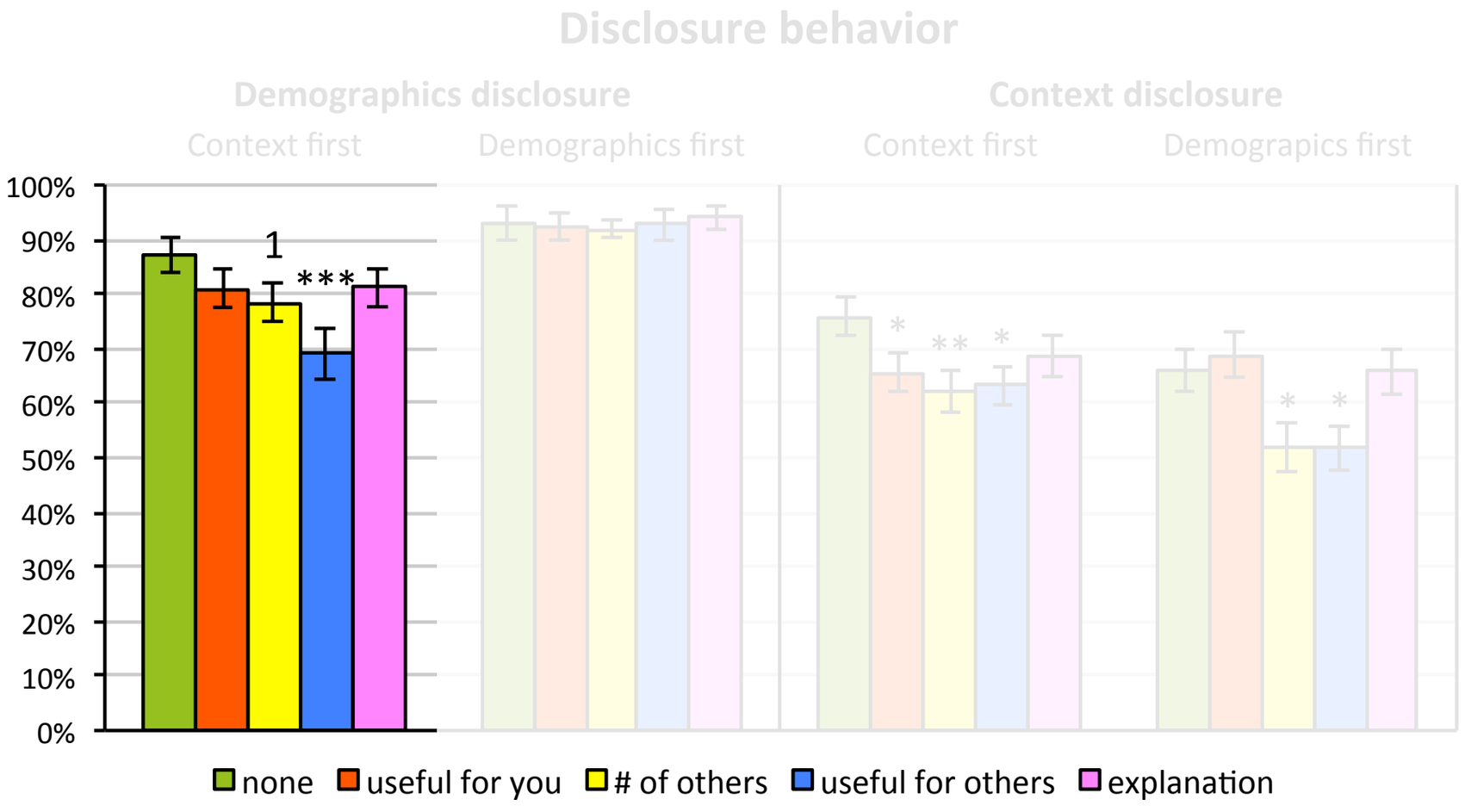
GENDER, ETC.

LOCATION, ETC.

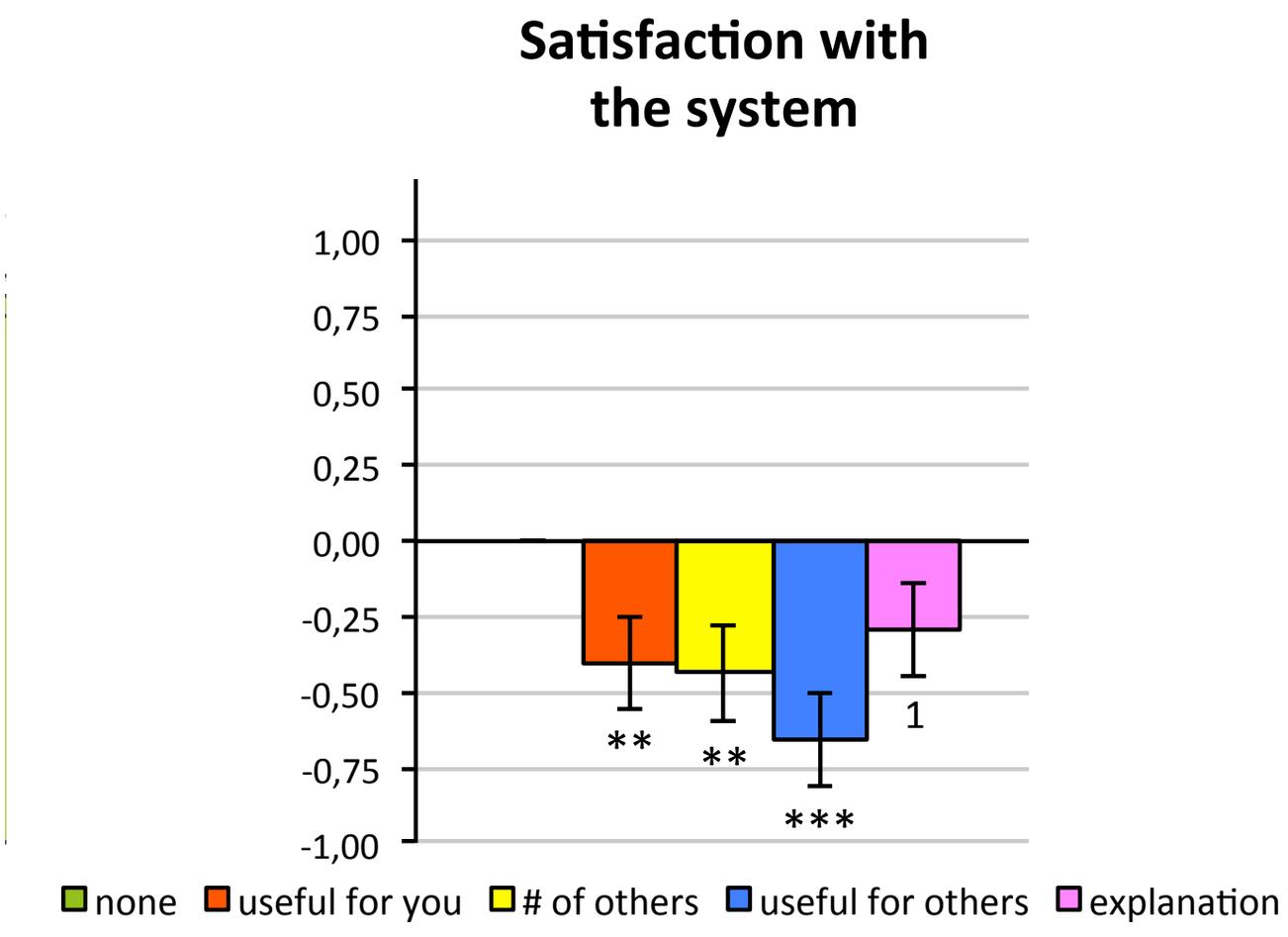
Asked first = more disclosure



Justifications don't work



Justifications don't work



Knijnenburg & Kobsa (2013) "Making Decisions About Privacy"

Nudge 3: Defaults/framing

Data: 14,729 household IoT-related scenarios + decisions from 1133 participants

Manipulate scenarios along 5 dimensions

Example scenario: "Your smart TV (Who) uses a camera (What) to give you timely alerts (Purpose), the data is stored locally (Storage) and used to optimize the service (Action)."

Nudge 3: Defaults/framing

Behavior: Allow/reject decision (see next slide)

Attitudes:

How expected/unexpected is this scenario?

How risky or safe is this scenario?

How useful/useless is this scenario to you?

How comfortable/uncomfortable do you feel about this scenario?

How appropriate/inappropriate do you consider this situation?

Nudge 3: Defaults/framing

Framing:

None: What would you do with this feature? (enable/disable)

Pos: Would you enable this feature? (yes/no)

Neg: Would you disable this feature? (no/yes)

Default option:

None: ○ enable ○ disable

Pos: ◉ enable ○ disable

None: ○ enable ◉ disable

Disclosure can be influenced

Defaults influence disclosure!

- Negative default: 1.37 times less likely to enable($p = .006$)
- Positive default: 2.57 times more likely to enable ($p < .001$)

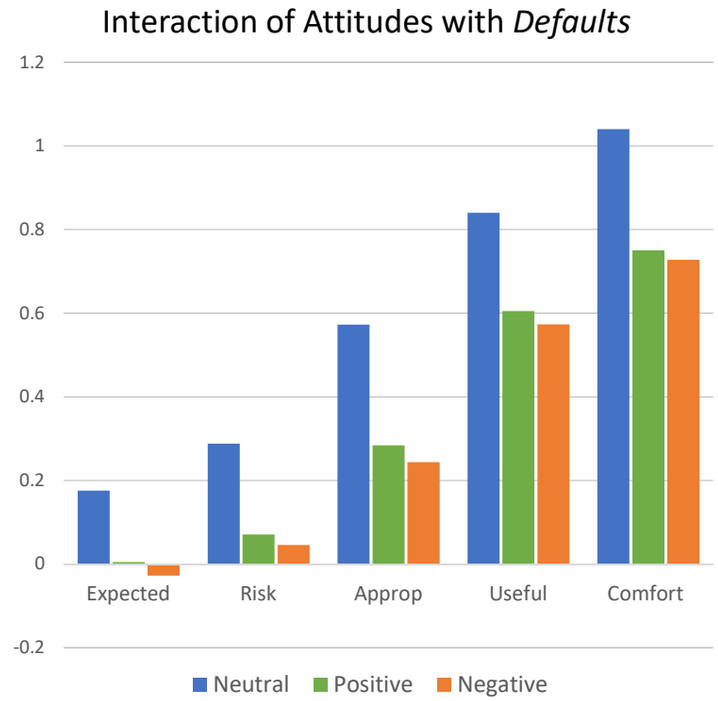
Framing too (but less)

- Negative framing: 1.31 times more likely to enable ($p = .0205$)
- No significant decrease for positive framing

Decision process deteriorates

However, they also **make people's decisions less nuanced!**

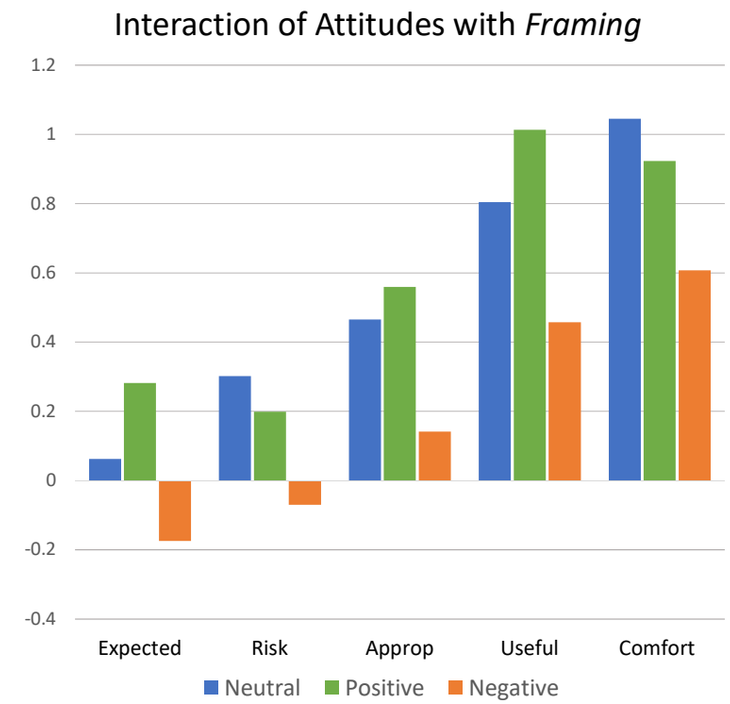
Defaults reduce the effect of attitudes on disclosure



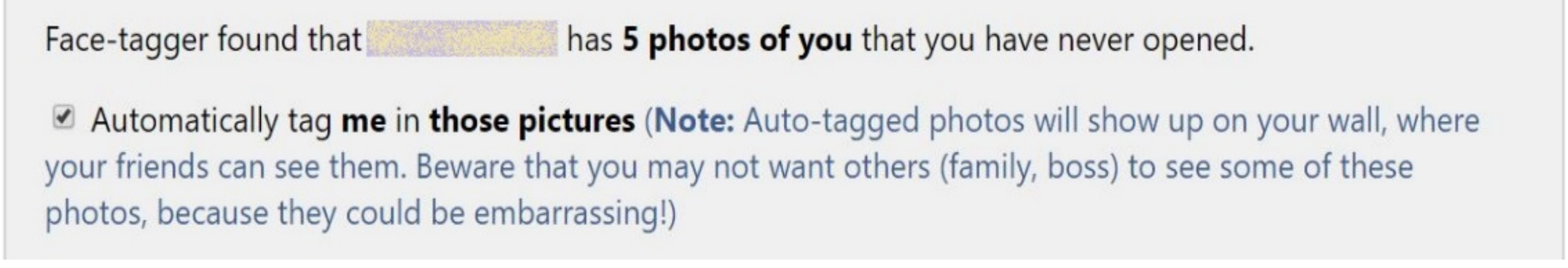
Framing also (kind of)

Negative framing reduces the effect of attitudes

Positive framing: certain attitudes have a stronger effect, others have a weaker effect

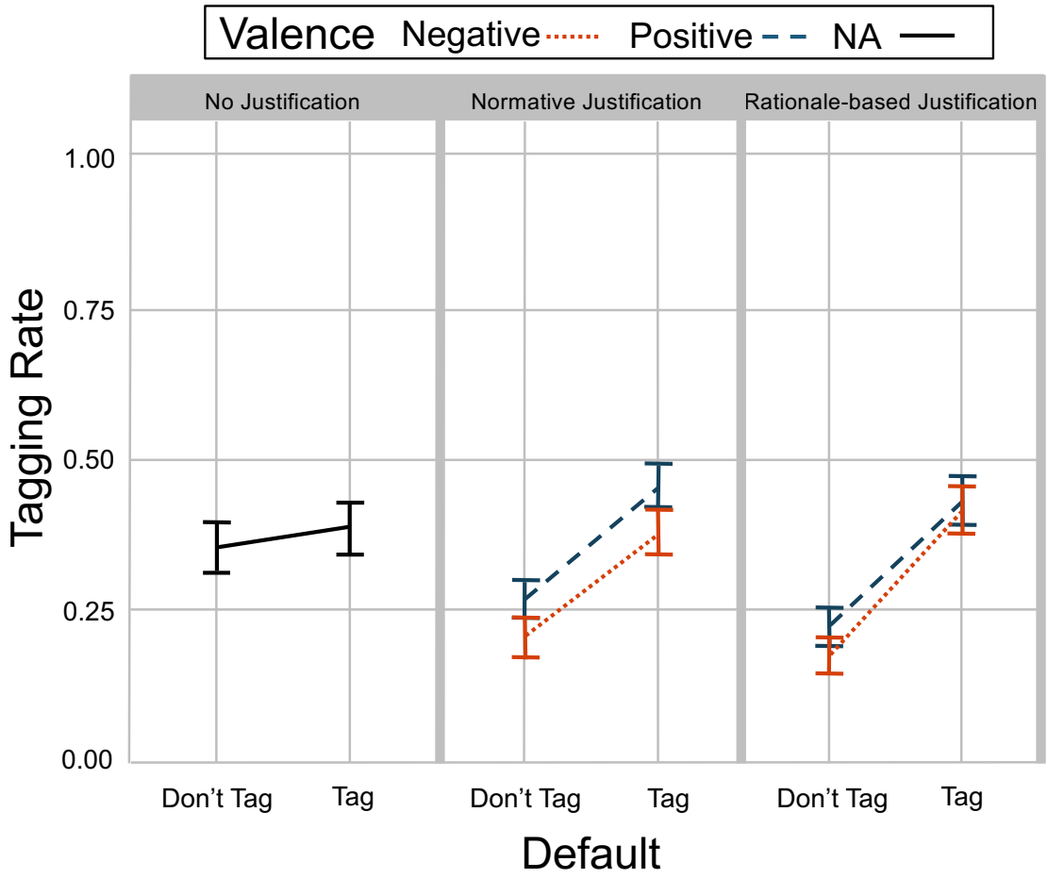


Combining them?



Adding justifications to defaults and framing exacerbates their effect!

In other words: justifications make people elaborate **even less**



Nudging does not work!

Conclusion: Nudges have unwanted side-effects

People are either annoyed by them…

…or they influence the decision process in unwanted ways.

Also, **how** should we nudge people?

Towards more privacy?

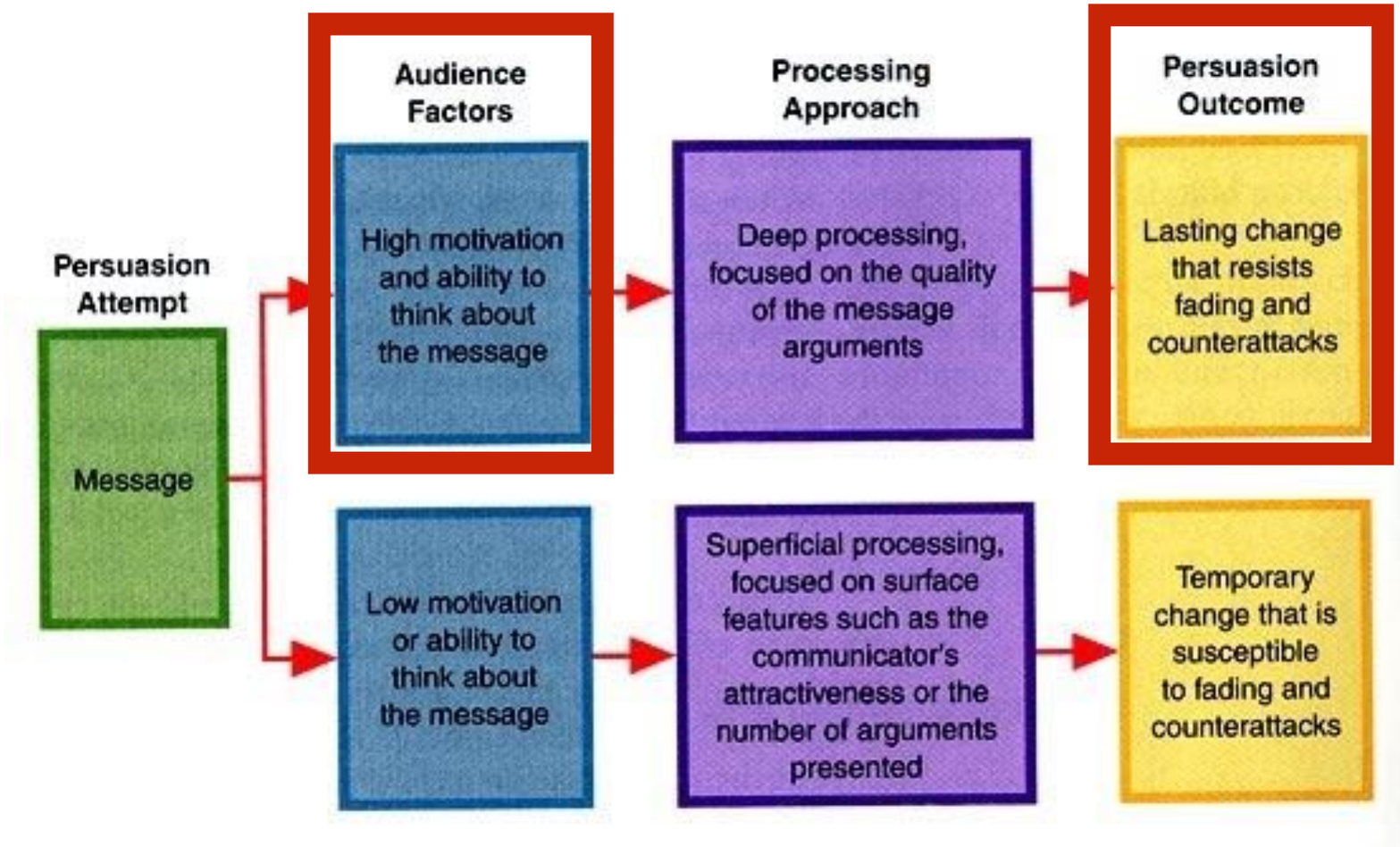
Towards more benefits?

The answer depends on the person and the context!

Design for elaboration

Making people think about privacy.

Dual-route processing



Kahneman (2013) "Thinking, fast and slow"

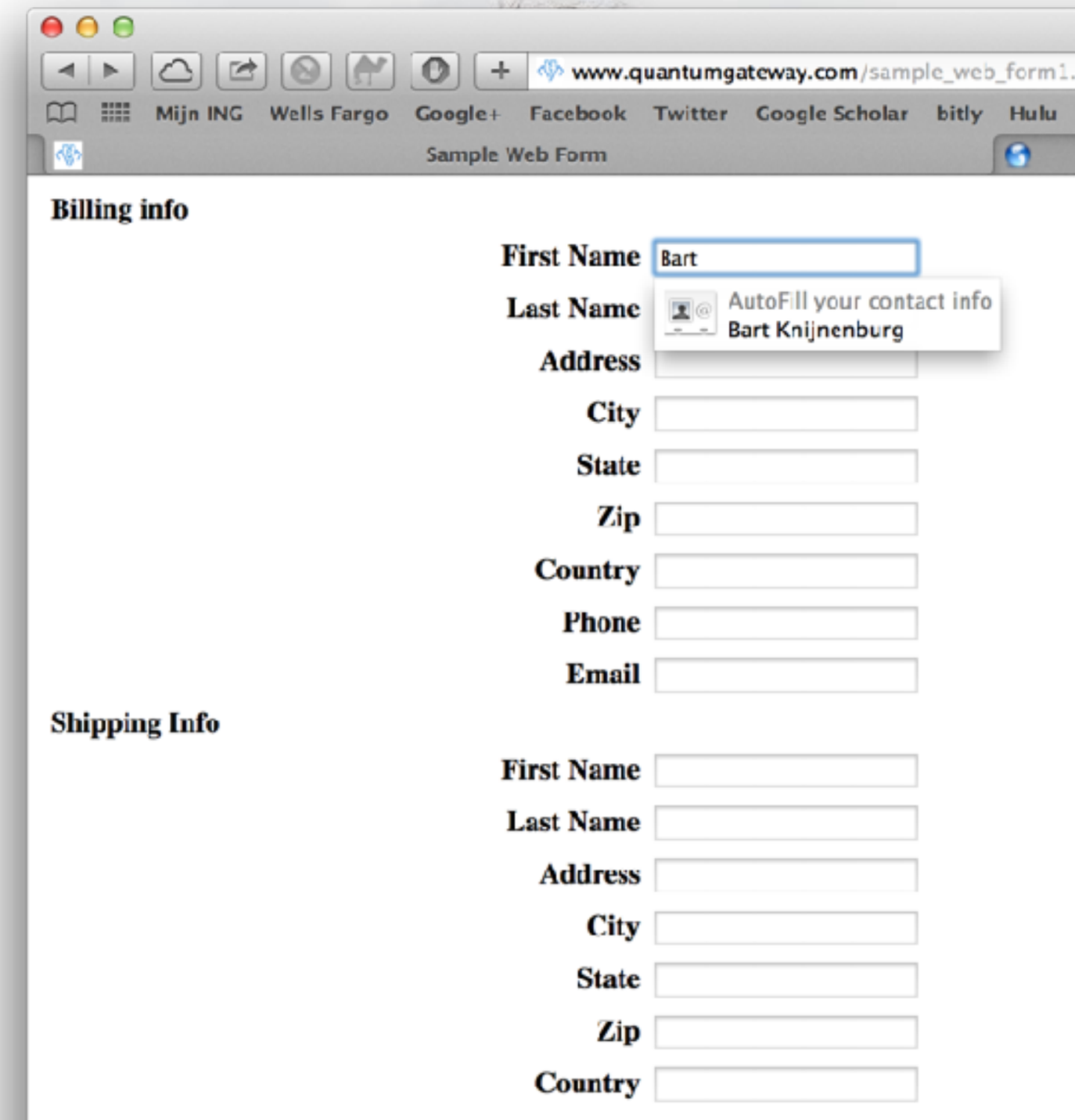
If we want lasting change, we must improve motivation and self-efficacy

Design for elaboration

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**



FormFiller

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:

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

Study Procedures

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:

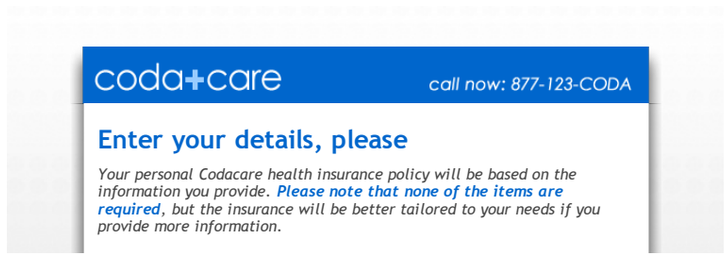
Tastes and Preferences:

Favorite movie:

Favorite band/artist:

Favorite food:

Favorite weekend pastime:



Study Procedures

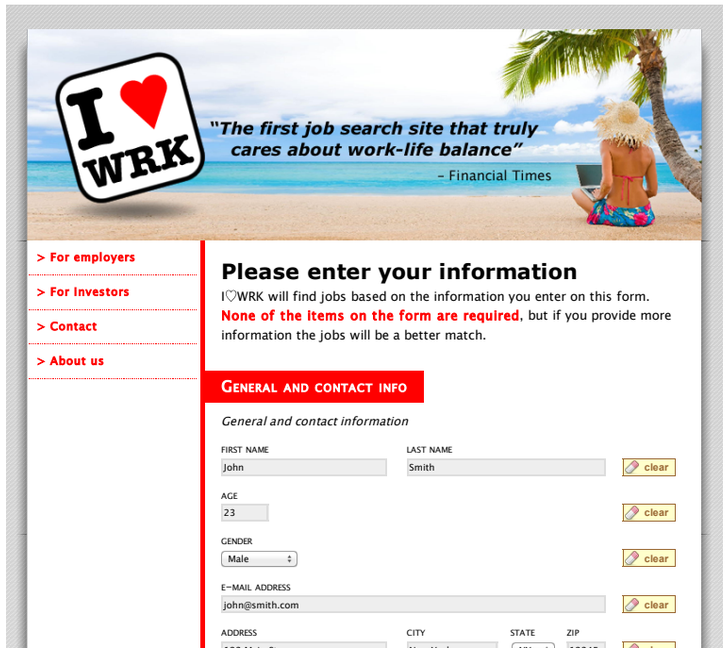
Each site corresponds to a particular type of info:

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!

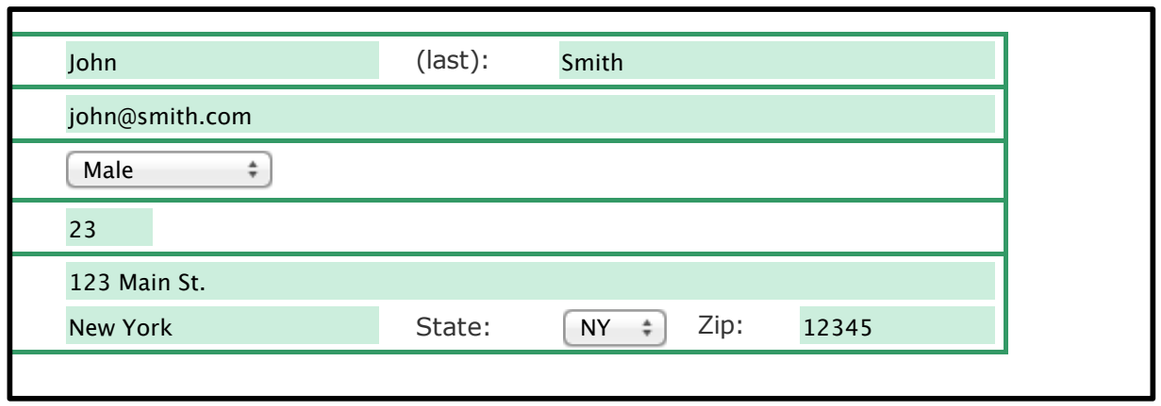


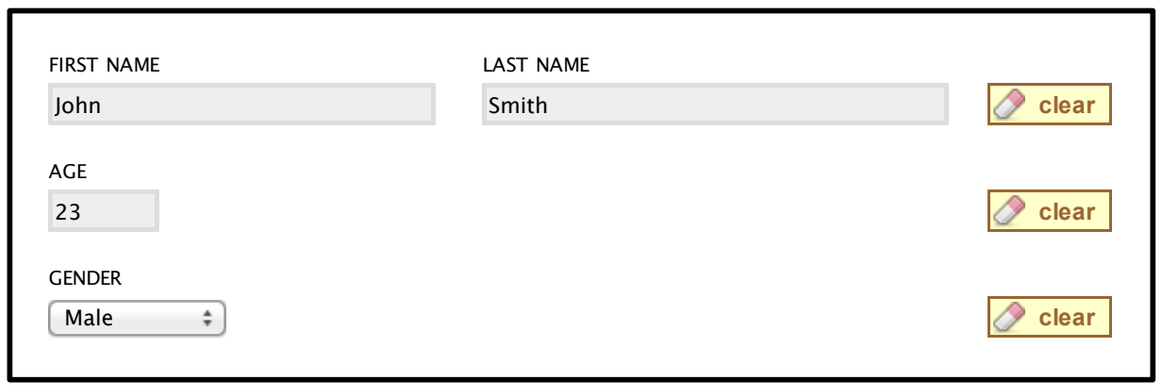
Research outline

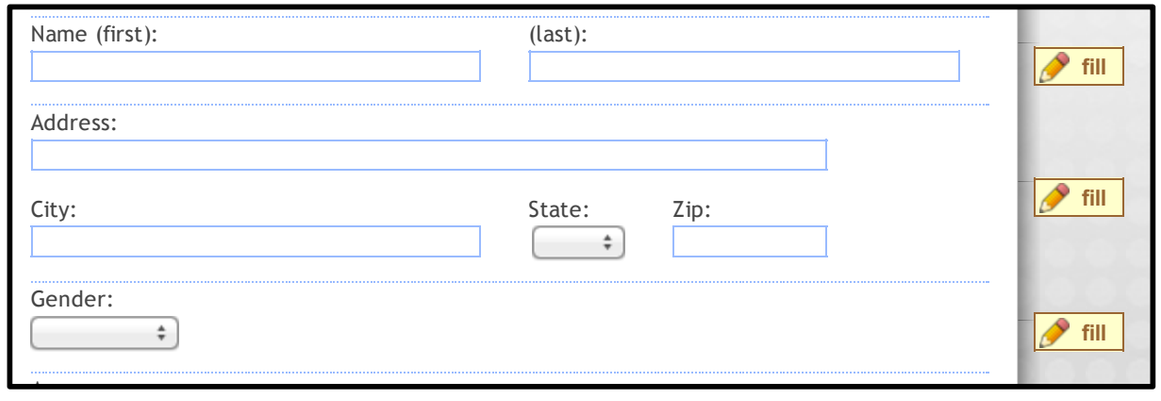
We introduce **two new efficacy-increasing designs**

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



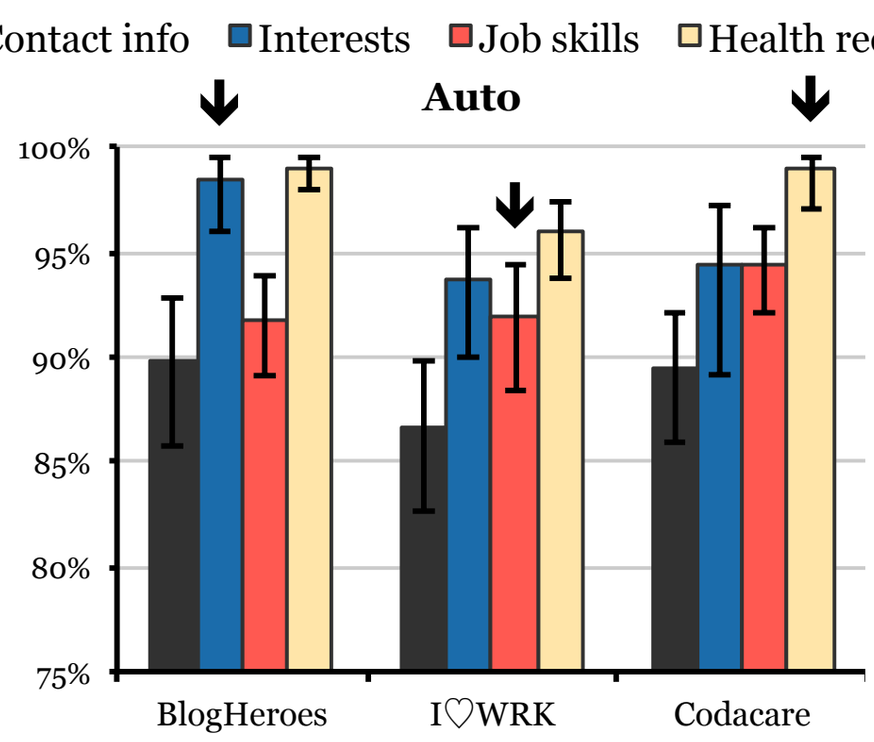


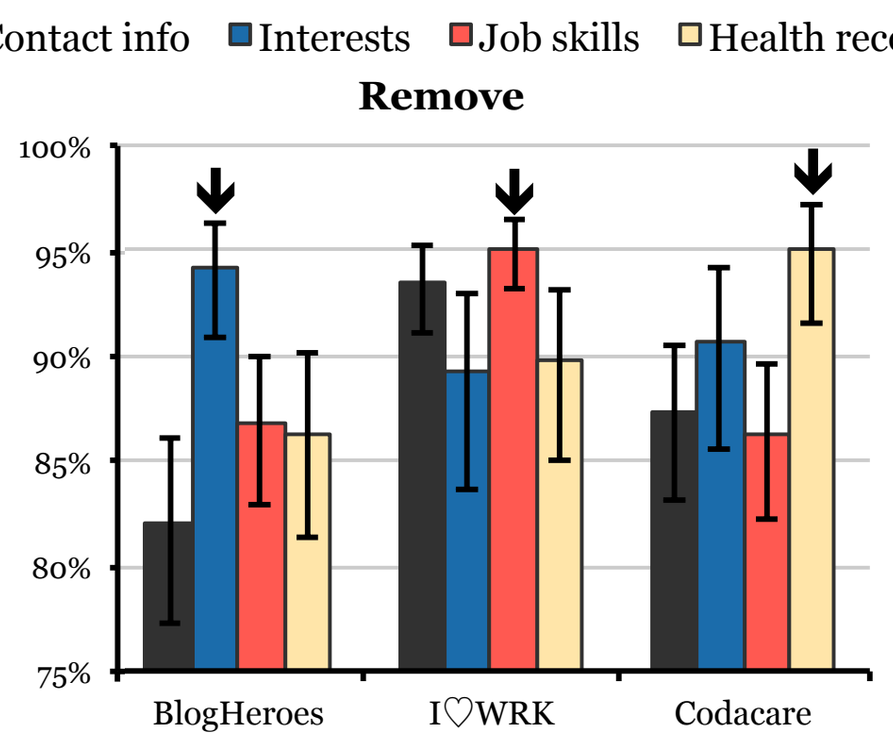


Design for elaboration

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. (2013) "Counteracting the Negative Effect of Form Auto-completion on the Privacy Calculus"

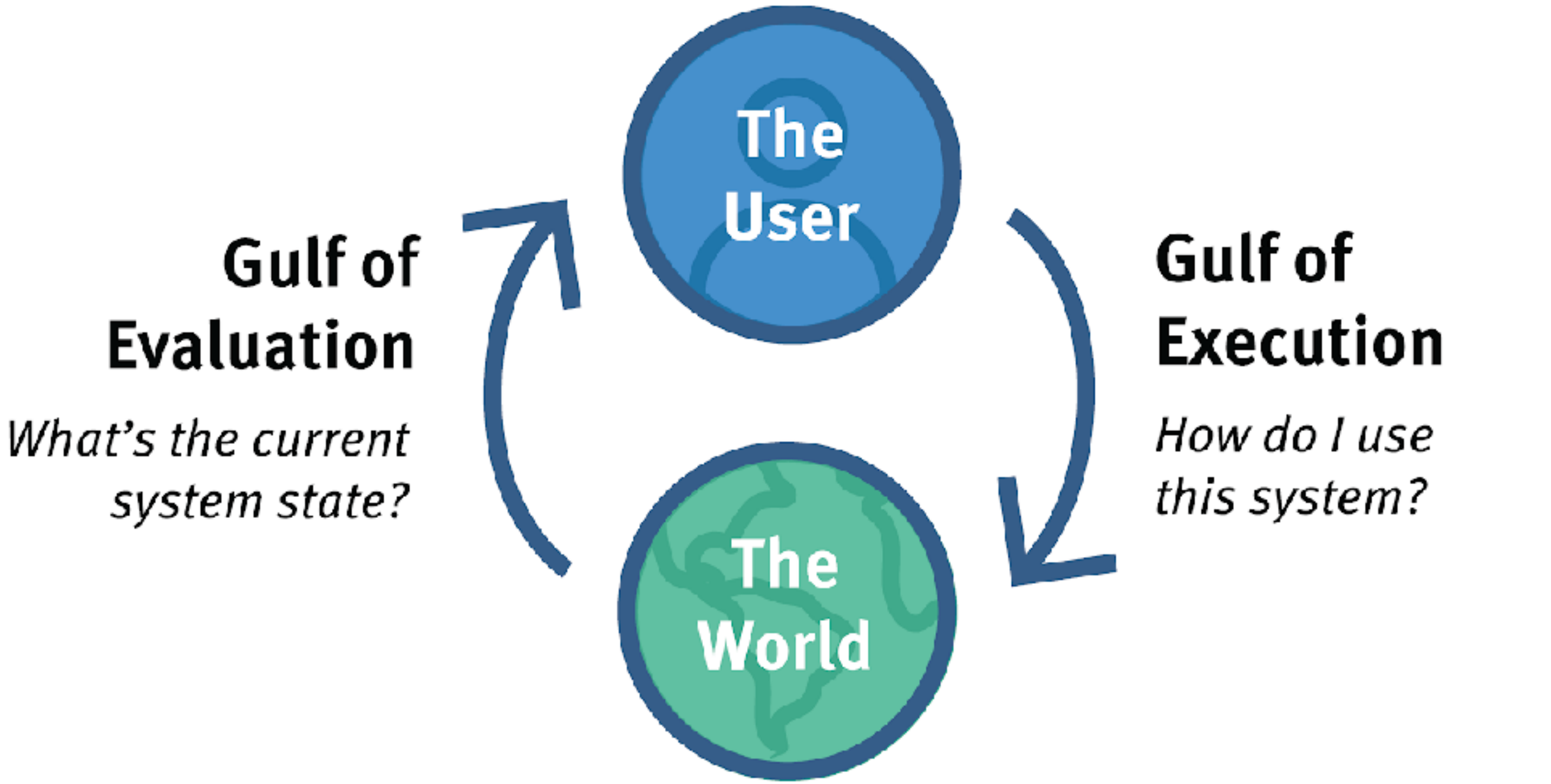
Privacy decisions are too hard!

Problem: Most systems are much too complex

- Privacy policies are increasing in length
- Facebook's privacy controls are "Labyrinthian"

It's easy to fall back on heuristic decision-making practices

- Which makes us fall prey to external influences such as defaults and framing


The User
Gulf of Evaluation
What's the current system state?
Gulf of Execution
How do I use this system?
The World

The Two UX Gulfs

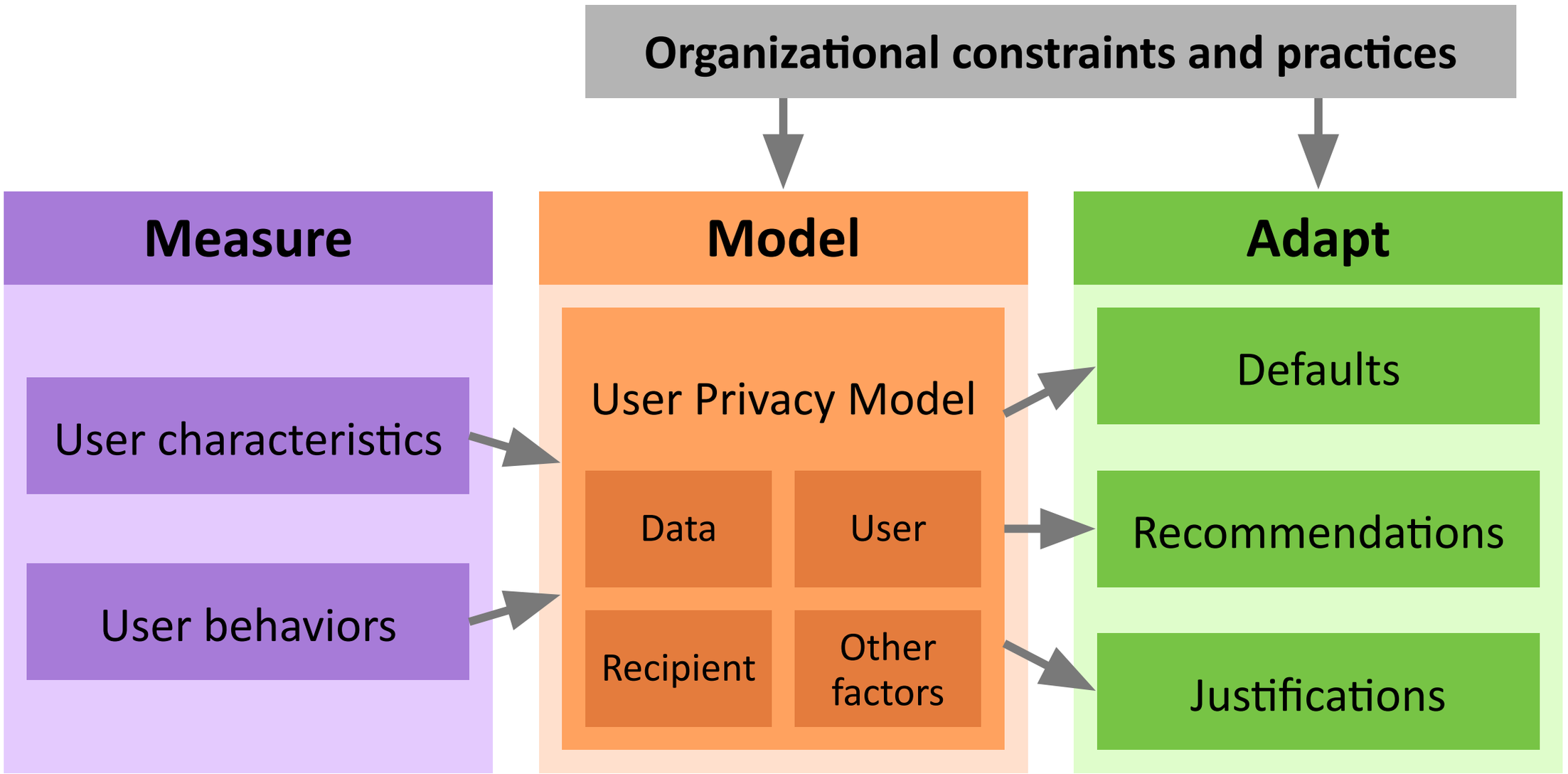
(Hutchins, Hollan & Norman 1986)

Users have difficulties translating their goals (desired privacy) into actions (settings).

User-Tailored Privacy

Privacy recommendations: Figure out what people want, then help them do that.

User-Tailored Privacy



Knijnenburg et al. (2022) "User-Tailored Privacy"

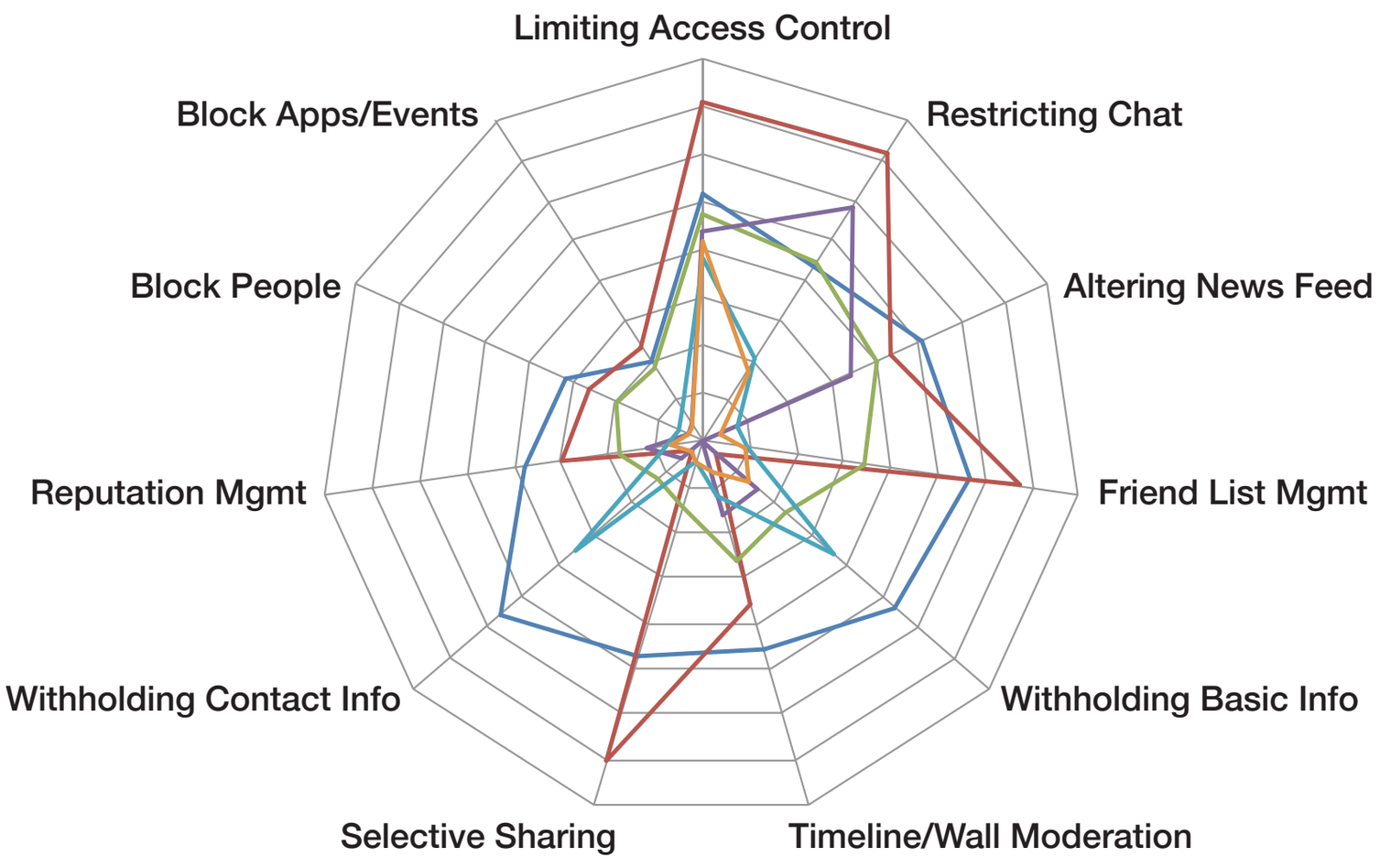
Use case:

Facebook privacy management practices

32 individual privacy behaviors that Facebook users could perform using the native Facebook interface

Create privacy profiles

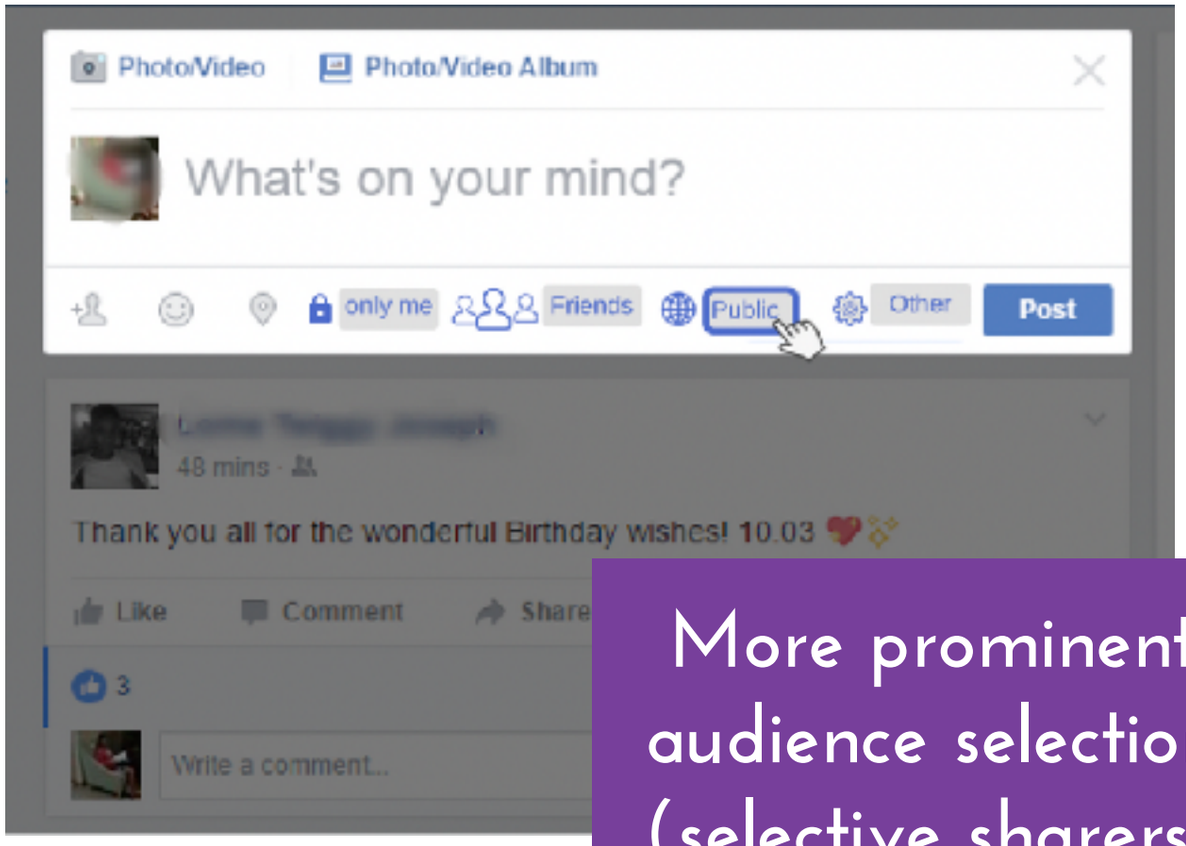
Privacy Maximizers | Selective Sharers | Privacy Balancers | Time Savers/Consumers | Self-Censors | Privacy Minimalists



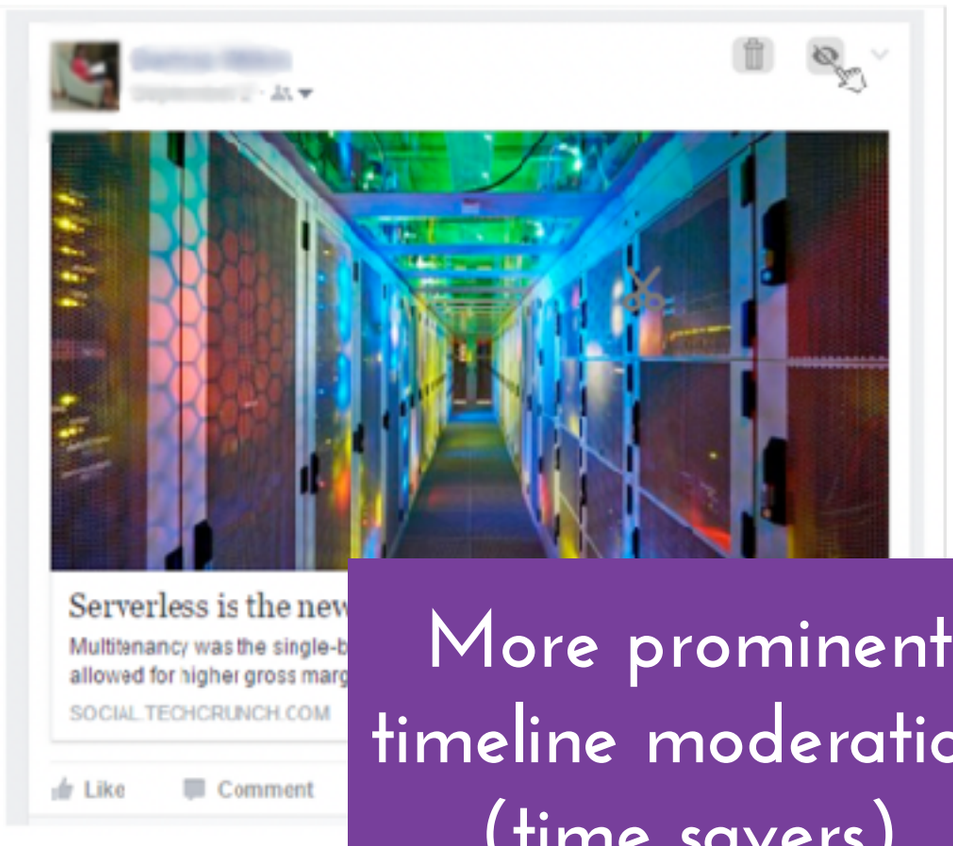
Wisniewski et al. (2017) "Making Privacy Personal"

see www.usabart.nl/chart

Adapt the interface



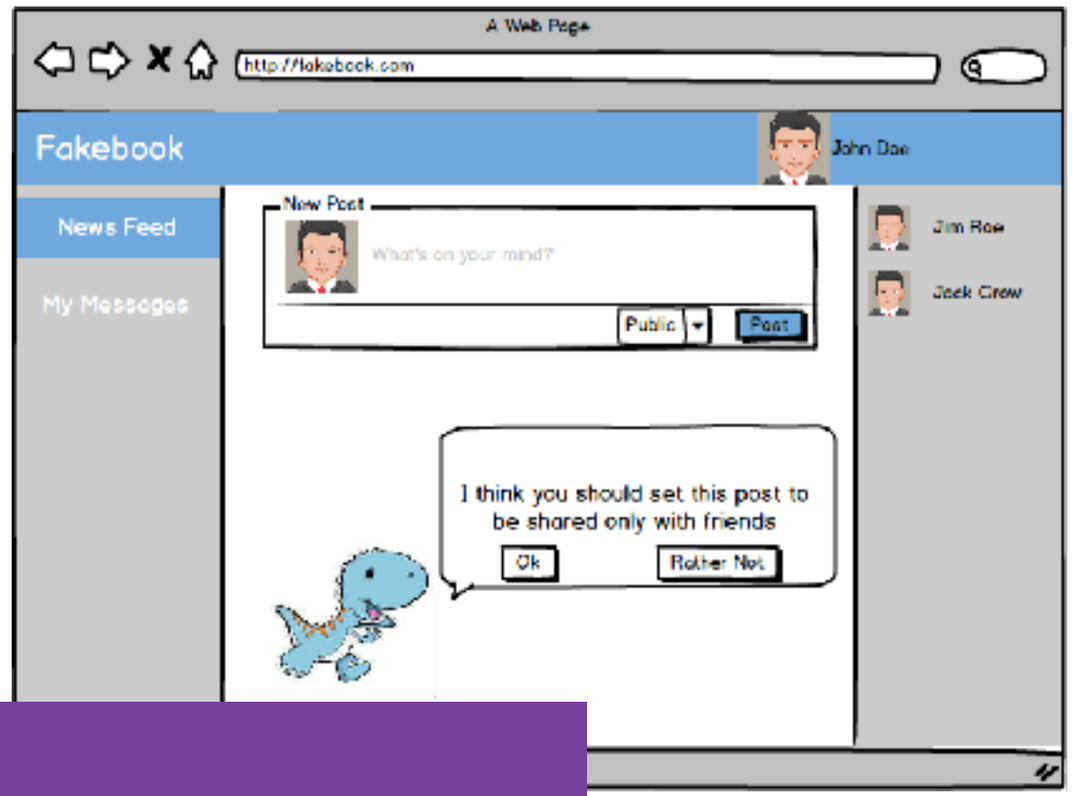
More prominent audience selection (selective sharers)



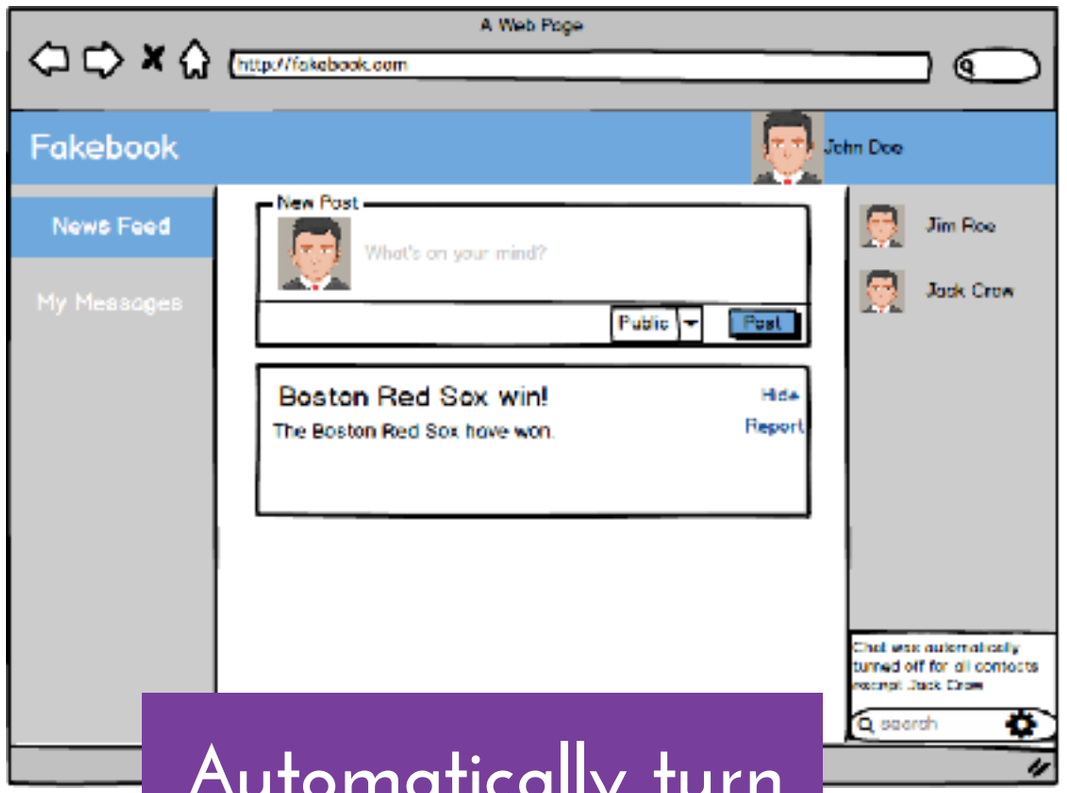
More prominent timeline moderation (time savers)

Wilkinson et al. (2017) "User-Tailored Privacy by Design"

Give recommendations



Audience suggestion (selective sharers)



Automatically turn off chat (time savers)

Namara et al. (2018) "The Potential for User-Tailored Privacy on Facebook"

Namara et al. (2022) "The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites"

Other adaptations

Adapt the nudge

Adapt the available options

Adapt the order of requests

Knijnenburg and Kobsa (2013)
"Helping users with information disclosure decisions: potential for adaptation"

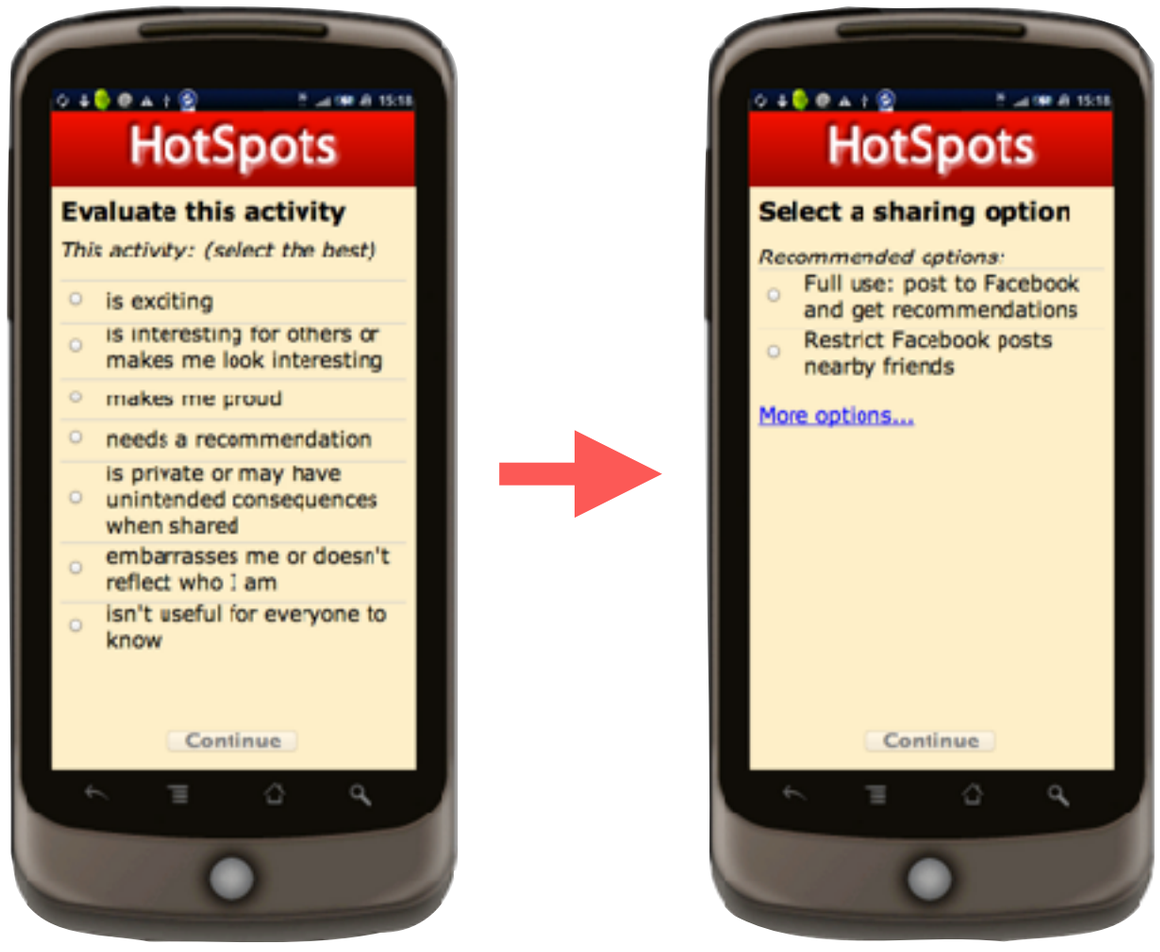
Other adaptations

Adapt the nudge

Adapt the available options

Adapt the order of requests

Knijnenburg and Jin (2013)
"The persuasive effect of privacy recommendations for location sharing services"



Other adaptations

Adapt the nudge

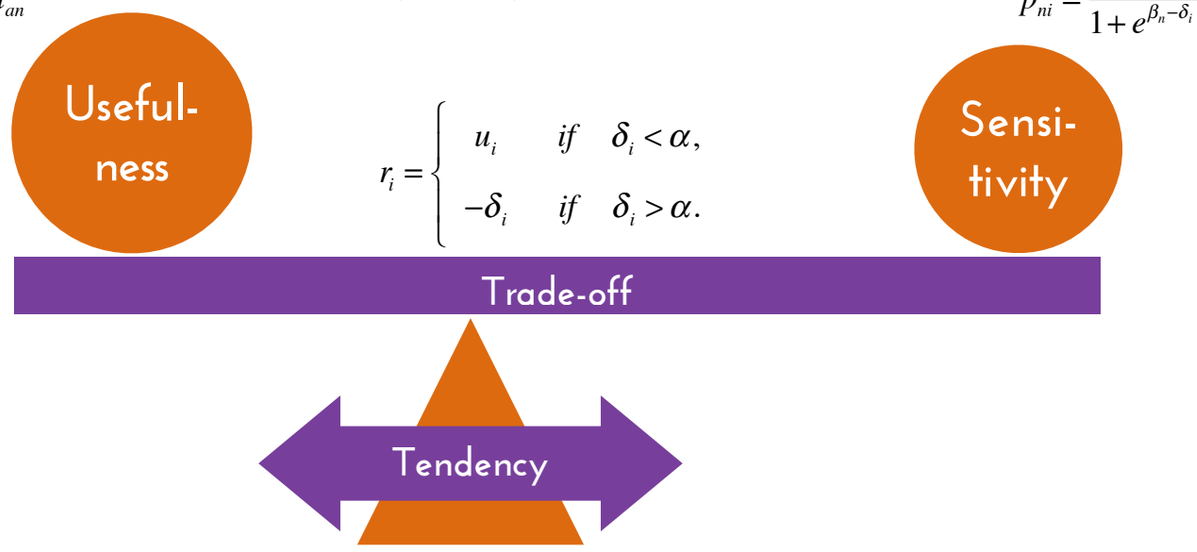
Adapt the available options

Adapt the order of requests

Knijnenburg (2015) "A user-tailored approach to privacy decision support"

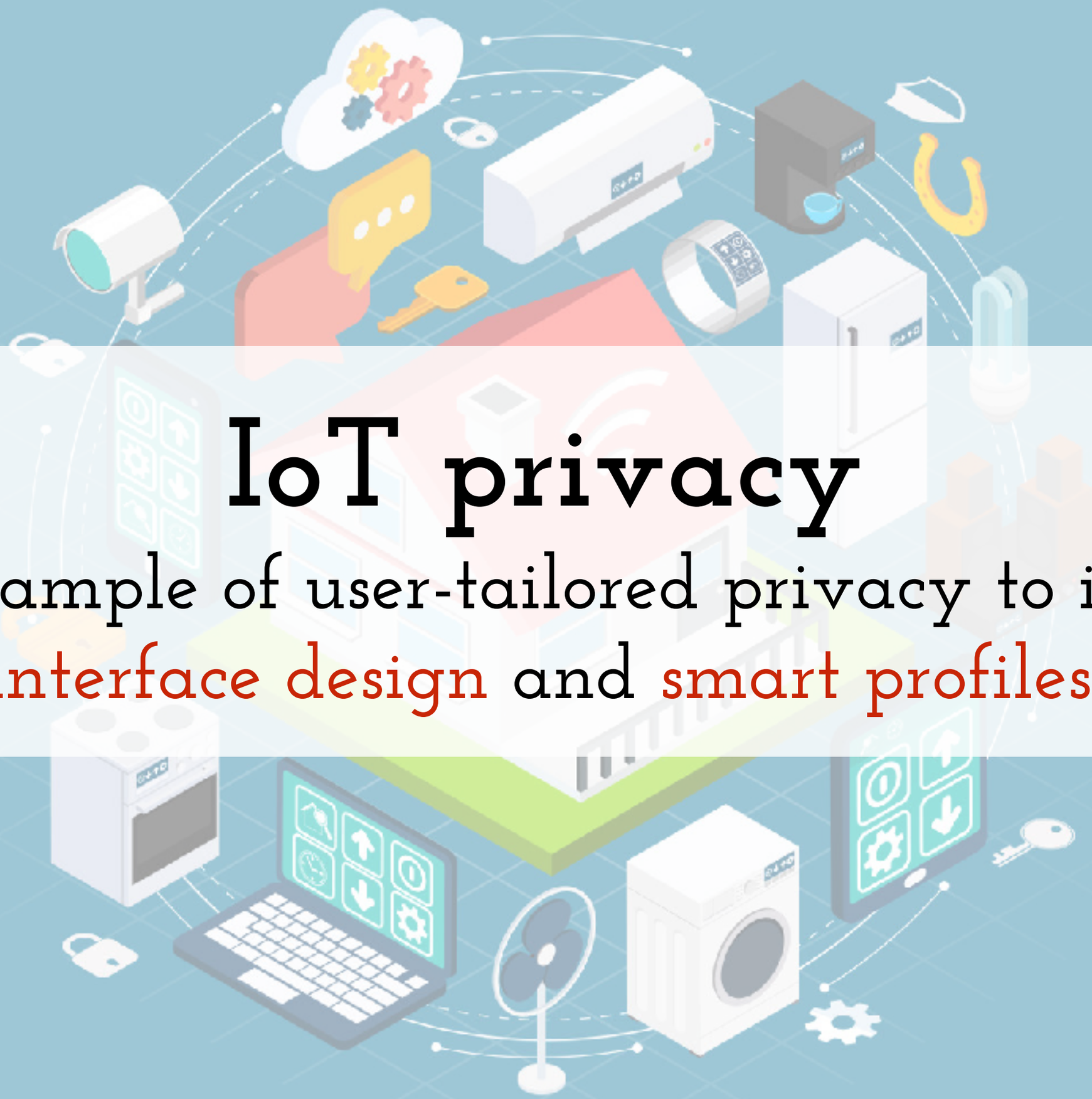
$$u_o = \sum_{r_{oa}} \frac{v_r}{d_{an}} \quad \text{where} \quad d_{an} = abs\left(w_{an} - \bar{w}_n\right) + .0001$$

$$p_{ni} = \frac{e^{\beta_n - \delta_i}}{1 + e^{\beta_n - \delta_i}}$$



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

$$\beta_n = \text{mean}_n(\delta) + \sqrt{1 + \text{var}_n(\delta)/2.9} * \ln\left(\frac{|D_n|}{|L_n| - |D_n|}\right) \quad \text{and} \quad \alpha_n^H = \beta_n - 1.5$$



IoT privacy

An example of user-tailored privacy to inspire interface design and smart profiles.

Use case:

2,800 public IoT-related scenarios + decisions from 200 participants

Manipulate scenarios along 5 dimensions

Example: "A device of a friend (who) records your video to detect your presence (what). This happens continuously (when), while you are at someone else's place (where), for your safety (why)."

Choice to allow or reject this scenario

Results

Let's say we create a layered settings interface

What parameter should be at the top?

What has the most influence on the user's decision?

Regression modeling to determine parameter order

Result: who > what > why > when > ~~where~~

Bahirat et al. (2018) "A data-driven approach to developing IoT privacy-setting interfaces"

9:00 AM 100%

Profiles

IoT Settings

Which **devices** may collect your personal information?

- My own devices — more
- Friends' devices — more
- Colleagues' devices — more
- Devices of nearby businesses — more
- My employer's devices — more
- Government devices — more
- Unknown devices — more

9:00 AM 100%

Settings

Friends' devices

What **type of data** may your friends' devices collect?

Voice, to determine my...

- age — more
- identity — more
- gender — more
- mood — more
- presence — more
- (other) — more

Photos, to determine my...

- age — more
- identity — more
- gender — more

9:00 AM 100%

Friends

Voice - age

For what **purpose** may your friends' devices record your voice to determine your age?

Safety

- **never** ✓
- once
- continuously

Health

- never
- **once** ✓
- continuously

Convenience

- **never** ✓
- once

Results

What about the default setting?

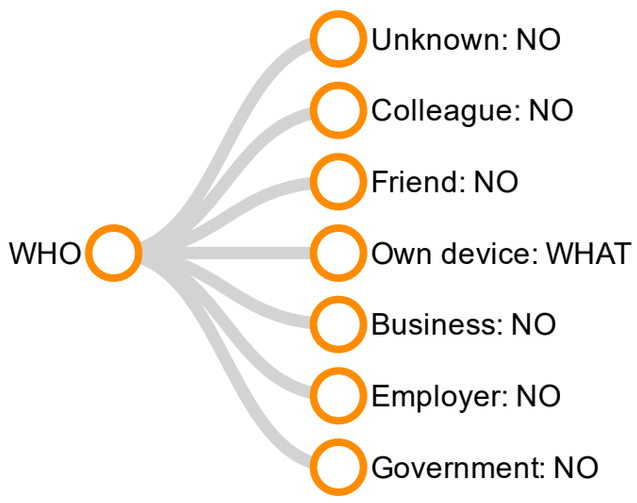
Everything on by default: 28% correct

Everything off by default: 72% correct

What if we make our best guess?

Predict based on who, what, where, when, why:

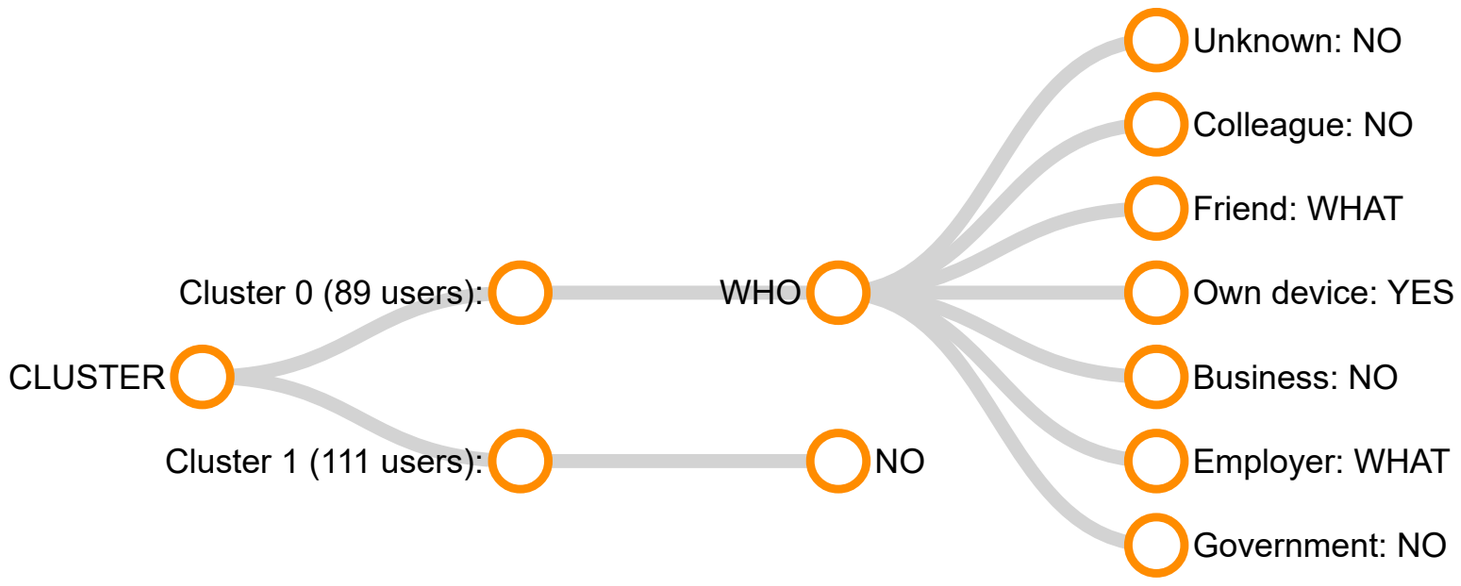
75% correct



Results

Divide participants based on overall attitudes?

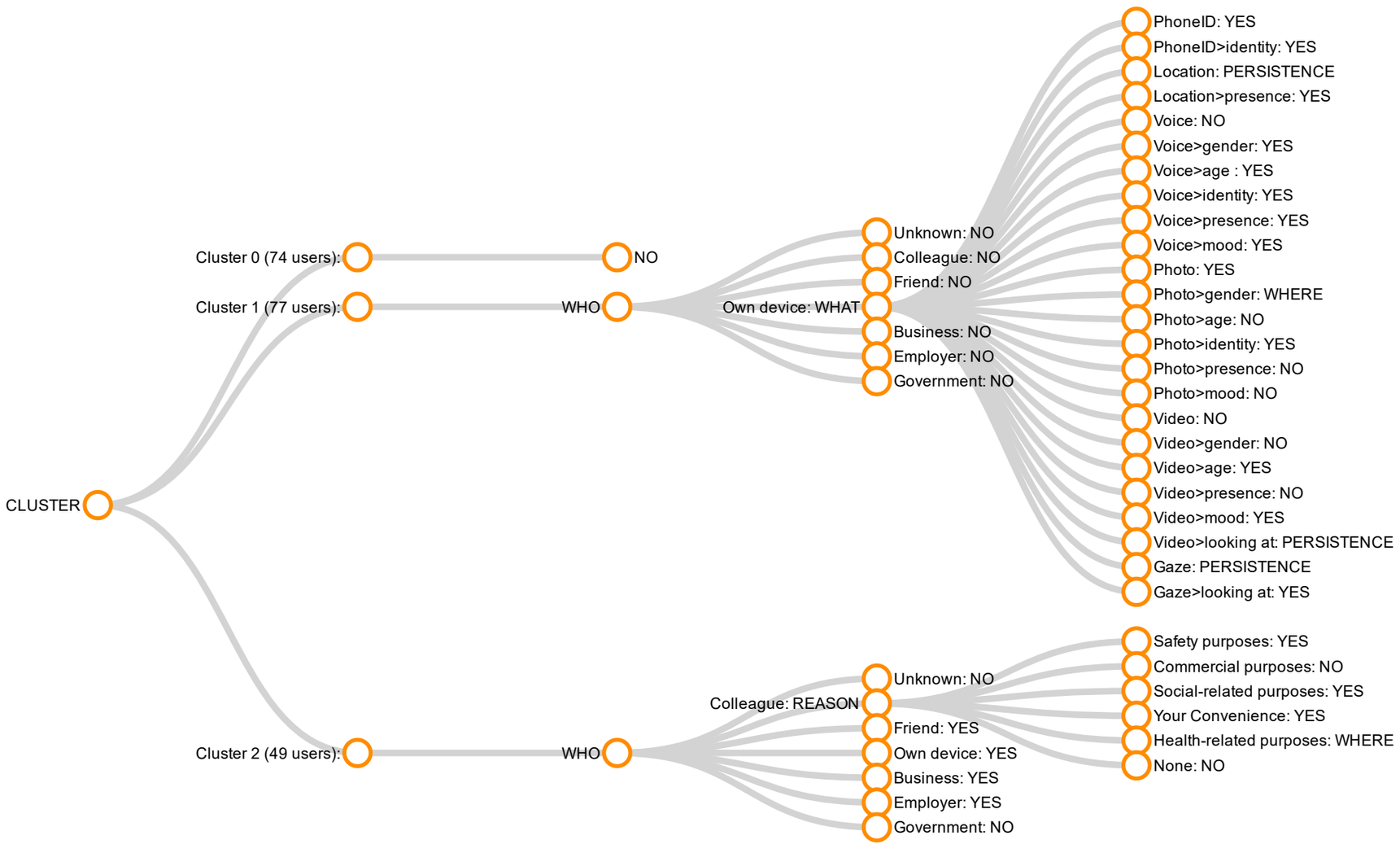
Two profiles: Correct 77% of the time!



Results

What if we divide participants on the fly?

Three profiles: Correct 82% of the time!



Step 1: choose a profile

Default profiles

Please select a profile
(you can change individual settings on the next screen)

Limited collection ✓

This profile allows the collection of:
- **any** data by the **your own devices**, your **friends' devices**, your **employer/school's devices**, and **devices of nearby businesses**
- **any** data by your **colleagues' devices**, but only for **certain reasons**

learn more...

Limited collection, personal devices only

This profile allows the collection of:
- **certain types** of data by the **your own devices**

No collection

This profile **prevents** the collection of **any** data

next >

9:00 AM 100%

< Profiles **IoT Settings**

Which **devices** may collect your personal information?

My own devices	on	more >
Friends' devices	on	more >
Colleagues' devices	off	more >
Devices of nearby businesses	off	more >
My employer's devices	off	more >
Government devices	off	more >
Unknown devices	off	more >

9:00 AM 100%

< Settings **Friends' devices**

What **type of data** may your friends' devices collect?

Voice, to determine my...

age	on	more >
identity	off	more >
gender	on	more >
mood	on	more >
presence	off	more >
(other)	off	more >

Photos, to determine my...

age	off	more >
identity	off	more >
	on	more >

9:00 AM 100%

< Friends **Voice - age**

For what **purpose** may your friends' devices record your voice to determine your age?

Safety

- **never** ✓
- once
- continuously

Health

- never
- **once** ✓
- continuously

Convenience

- **never** ✓
- once

Step 2: adjust the default settings

Conclusion

Next steps in usable privacy research.

My contribution

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

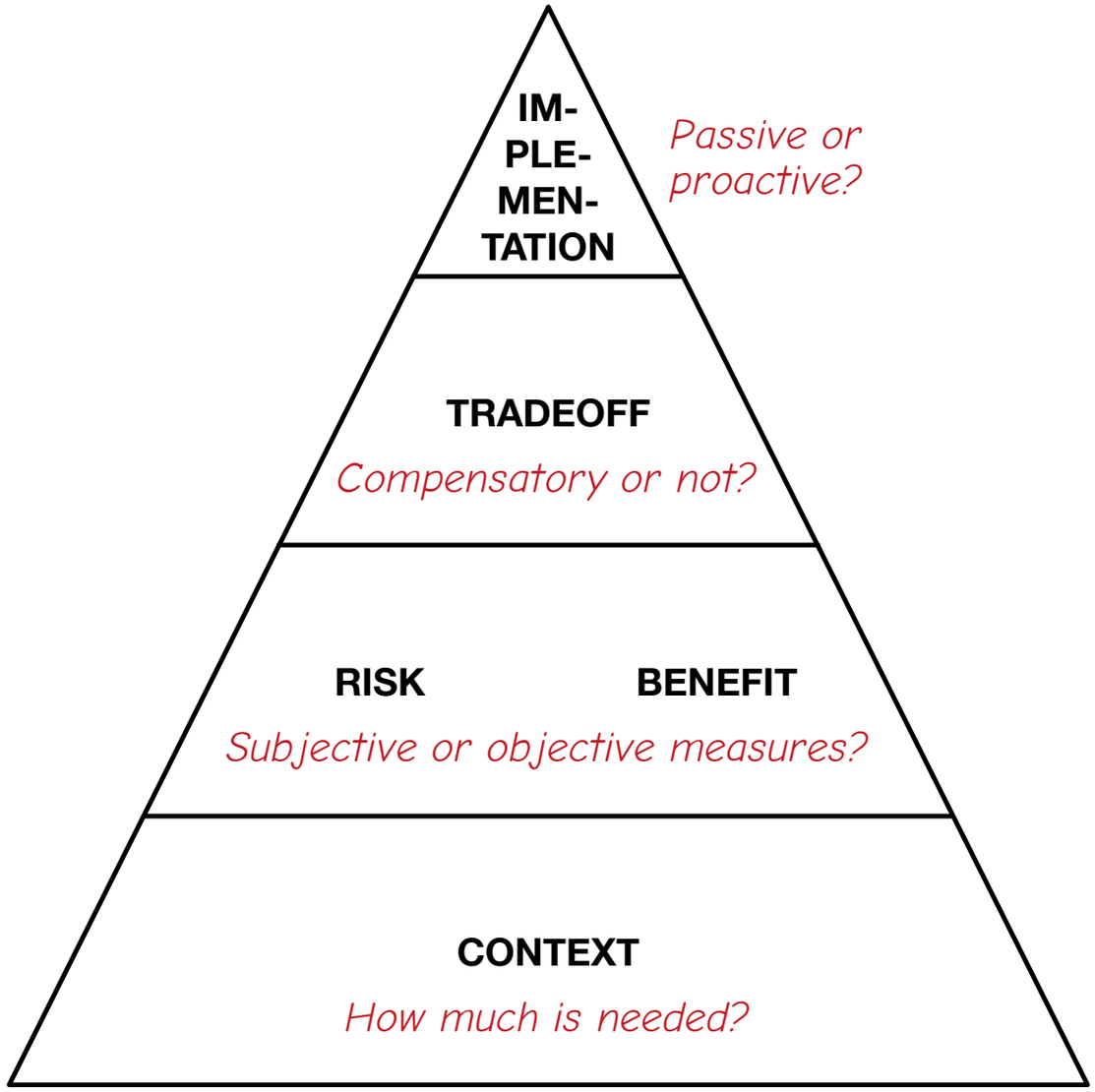
I presented the idea of "**design for elaboration**", which:

- Aims to increase **motivation** and **self-efficacy**, thereby encouraging people to **think slow**
- Nudges people to take control of their own privacy

I presented the idea of "**user-tailored privacy**", which:

- Provides **realistic empowerment** by relieving some of the burden of controlling privacy, while at the same time respecting each individual's preferences
- Refrains from making moral judgments about what the "right" level of privacy should be

Future research questions



Knijnenburg et al. (2017) "Death to the Privacy Calculus"