Session 3: Consumer Privacy Expectations
Your Data, My Decision: The Privacy Impact of Anonymous Sharing Across Varying Contexts

Jens Grossklags & Yu Pu
Interdependent Privacy

- To which degree do SNS users care about friends’ privacy? Are we good stewards of others’ data?
  - Many decisions on SNS involve data of “friends”
- Our scenario: Third-party Apps
Decision to adopt app

Data of user made accessible

Third-Party Company

1 User

Direct decision-making path

Data of 250 - 300 friends made accessible as well

Only very limited influence over decision
Approach

• Quantify the monetary value app users place on friends’ personal profiles on SNS
  – Measured with *conjoint analysis* method

• Survey constructs to develop behavioral model to explain valuations
  – Model built with *Structural Equation Modeling*
Experimental Treatments

Sharing Anonymity

Anonymous Sharing

Identifiable Sharing

Context Relevance

Irrelevant Context

Relevant Context
Effects of Sharing Anonymity and Context Relevance

Sharing Anonymity:  
\( p = 0.025 \)

Context Relevance:  
\( p = 0.002 \)

Detect the same effects for:  
- Friends' basic profile information
- Friends' valuable information
Value of Single Friend’s Data

Privacy Egoist

Data aggregated across treatments (same effects for different treatment groups)
Explain Interdependent Privacy Values

- PastPrivacy Invasion
  - TrustInApp: -0.21***
  - Privacy Knowledge: -0.27***
  - OtherRegarding Preference: 0.53***

- DispositionTo ValuePrivacy
  - OwnPrivacy Concern: 0.36***

- Perceived Control
  - OwnPrivacy Value: -0.05*

- OwnPrivacy Concern
  - FriendPrivacy Concern: 0.18
  - Sharing Anonymity: 0.18***
  - Context Relevance: 0.25***

- FriendPrivacy Value
  - Sharing Anonymity: -0.41
  - Context Relevance: -1.34*

* p < 0.05, ** p < 0.01, *** p < 0.001
Factors Driving Concern Towards **Own Privacy**

- **PastPrivacy Invasion**
  - $-0.21^{***}$
- **TrustInApp**
  - $-0.27^{***}$
  - $0.18^{***}$
- **DispositionTo ValuePrivacy**
  - $0.36^{***}$
- **Perceived Control**
  - $-0.05^{*}$
- **Privacy Knowledge**
  - $0.25^{***}$
- **OtherRegarding Preference**
  - $0.53^{***}$
- **FriendPrivacy Concern**
  - $0.58^{**}$
- **OwnPrivacy Concern**
  - $0.18$
- **OwnPrivacy Value**
  - $-0.41$
  - $-1.16^{**}$
- **Sharing Anonymity**
  - $-1.34^{*}$
- **Context Relevance**
  - $-1.82^{**}$

*p < 0.05, ** p < 0.01, *** p < 0.001*
Factors Driving Concern Towards Friends’ Privacy

-0.21***

TrustInApp

-0.27***

PastPrivacy Invasion

DispositionTo ValuePrivacy

0.36***

OwnPrivacy Concern

0.18

Perceived Control

-0.05*

Privacy Knowledge

0.18***

0.25***

OtherRegarding Preference

0.53***

FriendPrivacy Concern

0.58**

0.18

OwnPrivacy Value

-0.41

Sharing Anonymity

-0.16***

Context Relevance

-1.34*

-1.82**

*p < 0.05, **p < 0.01, ***p < 0.001
Factors Driving Privacy Valuation

- PastPrivacy Invasion
  - TrustInApp
    - Privacy Knowledge
      - OtherRegarding Preference
        - FriendPrivacy Concern
          - Sharing Anonymity
            - Context Relevance
          - FriendPrivacy Value
    - OwnPrivacy Concern
      - DispositionTo ValuePrivacy
        - Perceived Control
          - OwnPrivacy Value

* p <0.05, ** p < 0.01, *** p < 0.001
Lessons Learned - Policy

• App users are “privacy egoists”
  --> Limit the collection of friends’ data
    - What interventions are suitable?
    - Can app platforms (SNS) self-regulate interdependence?

• Privacy knowledge impacts interdependent privacy valuations
  --> Consider introducing policies which integrate interdependent privacy in educational programs
Lessons Learned – Privacy by ReDesign

• Data collection contexts affect how users value their friends’ information
  --> Call for mechanisms that inform users of apps’ data practices

• Sharing anonymity plays an important role in interdependent privacy valuations
  --> Suggests designs that inform users of whether sharing friends’ information will be later discoverable
Related Publications/Replications


It’s creepy, but it doesn’t bother me

Chanda Phelan, Cliff Lampe, Paul Resnick

University of Michigan

This research was funded by Google’s Social Interactions Focused Program
The intuitive process
System 1
• generates impressions
• automatic
• fast
• often emotionally charged

The reasoning process
System 2
• generates judgments
• conscious
• slower
• may be governed by logic
Intuitive concern
• emotional
• fast ("gut feeling")
• may not be able to articulate reasons

Considered concern
• assessment of how problematic
• may include explicit cost-benefit analysis
• doesn’t always happen
Interviewer: Would it change how you felt about [MT] if it read your messages?

S05: Oh, definitely. That’s pretty invasive.

Interviewer: What do you think is different?

S05: [pause] Good question. I don’t… [know] how to explain it. It’s just... I guess it's a matter of knowing who is going to see it. […] It would be kind of, just like... I don't know, it just kinda makes me less comfortable.
Factors
- Social presence
- Low marginal risk
- Trust

Intuitive
- Not creepy: Low intuitive concern

Creepy: High intuitive concern

Considered
- Bothered: High considered concern
- Not bothered: Low considered concern
"The fact that people know where I've been to [...] the fact that there's somebody behind me, trailing me, it's just a little scary." (S27)

“I don’t know. [...] it’s just like a weird thing to think about that someone’s sort of watching you, whatever you’re doing.” (S04)
“The fact that people know where I've been to [...] the fact that there's somebody behind me, trailing me, it's just a little scary.” (S27)

“I don’t know. [...] it’s just like a weird thing to think about that someone’s sort of watching you, whatever you’re doing.” (S04)
Factor: Social presence

Social presence

Intuitive
- Not creepy: Low intuitive

Creepy: High intuitive

Considered
- Bothered: High considered
- Not bothered: Low considered
“All you guys were asking for was monitoring my sites and my hits, and basically a lot of other sites already do that without my permission.” (S30)

“I'm just numb to the fact that people can get information about me. I guess, it did occur to me like, ‘Oh, what if they can see my Facebook?’ […] [but in the end] I just signed up for it.” (S11)
“All you guys were asking for was monitoring my sites and my hits, and basically a lot of other sites already do that without my permission.” (S30)

“I'm just numb to the fact that people can get information about me. I guess, it did occur to me like, ‘Oh, what if they can see my Facebook?’ […] [but in the end] I just signed up for it.” (S11)
Factor: Low marginal risk

- Intuitive: Not creepy: Low intuitive
- Creepy: High intuitive
- Considered: Bothered: High considered
- Not bothered: Low considered
“I was just flipping through, yay, whatever, install, and then when I went and looked back […] I was like, ‘Wow. They must be collecting something in my computer.’ […] So, I guess I was maybe hesitant […] I feel like that's not their motive, to collect personal information from me. […] Especially when it's coming from professors from the university, they’re trustworthy people.” (S08)
Factor: Trust

“I was just flipping through, yay, whatever, install, and then when I went and looked back […] I was like, ‘Wow. They must be collecting something in my computer.’ […] So, I guess I was maybe hesitant […] I feel like that's not their motive, to collect personal information from me. […] Especially when it's coming from professors from the university, they’re trustworthy people.” (S08)
Factor: Trust

- Intuitive:
  - Not creepy: Low intuitive

- Creepy: High intuitive

- Considered:
  - Bothered: High considered
  - Not bothered: Low considered
Factors

Intuitive

Creepy: High intuitive concern

Considered

Bothered: High considered concern

Not bothered: Low considered concern

Not creepy: Low intuitive concern
1) **Existing** explanation of the privacy paradox

- **Intuitive**
  - Not creepy: *Low intuitive concern*
  - Creepy: *High intuitive concern*

- **Considered**
  - Bothered: *High considered concern*
  - Not bothered: *Low considered concern*

Factors
2) **New** explanation of the privacy paradox

- **Intuitive**
  - Not creepy: Low intuitive concern
  - Creepy: *High intuitive concern*

- **Considered**
  - Not bothered: Low considered concern
  - Bothered: *High considered concern*
Practical Policy Implication: Focus on Considered Concern

- Elicit only considered concern
- Encourage congruence
  - If low considered concern, encourage product owners to reduce intuitive concern
  - If high considered concern, prevent product owners from reducing intuitive concern
Folk Models of Online Behavioral Advertising

Yang Wang
Syracuse University

This research was funded by National Science Foundation (#1464347)
Online behavioral advertising (OBA)

“Tracking a person’s online activities in order to deliver advertising tailored to the person’s interests”

People have mixed feelings about OBA

Don’t know what people think about how OBA works
Folk model

Models of reality used to reason and make decisions

Can be incorrect but are used by people in practice

Source: medium.com
Why folk models matter?

Understand *user attitudes*

Customize *user education*

Influence *user behavior*
Interviews

2 rounds of interviews
- How OBA works
- Information vs. trackers
- Privacy tools for OBA

21 participants
- New York, California
- Age: 18-64 (avg. 34)
- Gender: 6 F, 15 M
Hypothetical scenario

You first look for shoes on Amazon.com and a few hours later you visit Facebook and see other shoe ads there
Browser-Pull

Browser does it all

I'm searching for shoes on Amazon.

I switch to Facebook.

Ad for Amazon.

Web browser tracks my activity.

Amazon has contract w/ browser to sniff ads.
1st Party-Pull

Browser tracks and stores user info

1st-party sites pull ads
Connected 1<sup>st</sup> Party

1<sup>st</sup> party does it all

1<sup>st</sup> party shares directly
3rd Party

3rd party does it all
Common practice

![Diagram showing relationships between Amazon, Facebook, and third party tracker]
Information being tracked more important than who’s tracking it (i.e. trackers)

“I mean the biggest thing is the information. I mean trackers are replaceable, but information is not because that’s a specific set of info per person.”
Implications for design and policy

Tools cannot assume users know about 3\textsuperscript{rd} parties

Trackers \textbf{should} clearly explain data they collect

Information-based vs tracker-based blocking
Acknowledgements

Joint work with Yaxing Yao and Davide Lo Re

What Is Online Tracking?

Cookies are small tokens that store website state
• Used for: logging in, shopping carts, tracking

User requests web page

User ID is 1234

1st Party
What Is Online Tracking?

Later...

User loads another web page on the same domain

My user ID is 1234

Custom content

1st Party
What Is Online Tracking?

Later...

User loads another web page on the same domain

My user ID is 1234

Custom content

Ad for CNN; ID for advertiser: 5678

Ad

1st Party

3rd Party

User

The New York Times

PrivacyCON
What do experts think about online tracking?

**Proponents say:**
- Targeted (better) ads, customized content, social widgets, shopping recommendations
- Revenue used to provide free services online

**Opponents say:**
- Privacy concerns
- Third parties can build detailed profiles about users
- Can happen without users’ knowledge
But What Do *Users* Think?
Current Understanding of Users’ Views

• 65% to 79% have serious privacy concerns
• Users’ preferences are complex
• But, prior studies mostly in hypothetical scenarios

How do you feel about tracking ... ... when you were shopping for heartburn medicine on Thursday on amazon.com?

... on a shopping website? vs
Research Questions

In the context of users’ own web history:

• What harms and benefits do users care about?
• What situational factors affect users’ comfort with tracking?
• Do current tools address users’ needs?
• How can we improve current tools?
Methodology

- 35 semi-structured interviews
- Variety of situations:
  - News, weather, shopping, search, financial services, etc.
  - 1st and 3rd party tracking
- Two coders developed codebook and coded interviews

Prepare interview → Send filtered web history → Conduct interview
Methodology: Example Situation

For your *nytimes* visit:

- Benefits of tracking?
- Harms of tracking?
- Are you comfortable with tracking?

1. nytimes.com
The New York Times - Breaking News on Wed, Jan 14 07:05 PM
Results

- Perceived outcomes of tracking
- Situational factors
Example Perceived Outcomes: Overt

- Targeted ads
  - Beneficial: more useful, relevant
  - Harmful: annoying, others might see
- Feel “stalked”
- Customized websites
  - Beneficial: saves time, more relevant
  - Harmful: “filter bubble”
Example Perceived Outcomes: Hidden

- **Company revenue**
  - Beneficial: provides for free services
  - Harmful: feel used by companies
- **Price discrimination**
  - Beneficial: special sales, coupons
  - Harmful: maybe higher prices
- **Data linked to identity**
  - Harmful: privacy invasive

(Bar chart showing percentage of participants' views on each outcome.)
Outcomes vs. Comfort

- Perceived harms/benefits → comfort
- Less comfortable with harms
- Hidden outcomes → least comfortable
Situational Preferences

What about specific page visits made users more or less comfortable?

- Sensitive contexts: less comfortable with 3rd party tracking than 1st
- What kind of information is tracked
- Sharing with other 1st parties
- Trust in the tracking party
- Lack of awareness of tracking
- Lack of consent to tracking
- Visit frequency to website
Tool Evaluation

• Use findings from interviews to evaluate tools
  ✓ Adequately address perceived harms
  ✗ Do not allow benefits
  ✗ Provide few controls based on situational factors
Does More Detailed Understanding of Preferences Lead to Better Tools to Control Tracking?
Situational Preference Prediction

Use machine learning methods to predict comfort with tracking for a specific page visit from situational factors.

- User predicted as uncomfortable
- Block tracking

- User predicted as comfortable
- Allow tracking
Prediction Accuracy

% of good tracking allowed vs % of bad tracking allowed

Ideal
Prediction Accuracy
(Do Not) Track Me Sometimes

- Explored users’ \textit{in-context} preferences
  - Based on actual browsing history
  - Found outcomes, situational factors that matter
- Evaluated current tools
  - Tools don’t adequately address users’ needs
- Hope for automated preference enforcement
Discussion of Session 3

Presenters:
• Jens Grossklags, Technical University of Munich
• Yu Pu, The Pennsylvania State University
• Chanda Phelan, University of Michigan School of Information
• Yang Wang, Syracuse University
• Mahmood Sharif, Carnegie Mellon University

Moderator:
• Lorrie Cranor, Federal Trade Commission
LUNCH POSTER SESSION