Human-centered privacy foundations

CS 7375: Seminar: Human-Centered Privacy Design and Systems (co-located with PHIL 5110)

Tianshi Li | Assistant Professor

Announcements

- Project feedback has been released!
- The project proposal assignment has been released (due **next Wednesday midnight**)
- Reading commentaries due this Wednesday noon

Agenda

- How does “humanness” contribute to privacy problems? Suboptimal privacy behaviors, Awareness, Mental Model, Cognitive Load, Incentives, concerns, privacy preferences etc.
- Paradigms of human-centered privacy research and research methods

Human is the weakest link in Cybersecurity

Do people follow good privacy practices?

image source: https://theferrarigroup.com/once-again-the-weakest-link-in-the-supply-chain-has-lasting-impact/

Excessive online disclosure

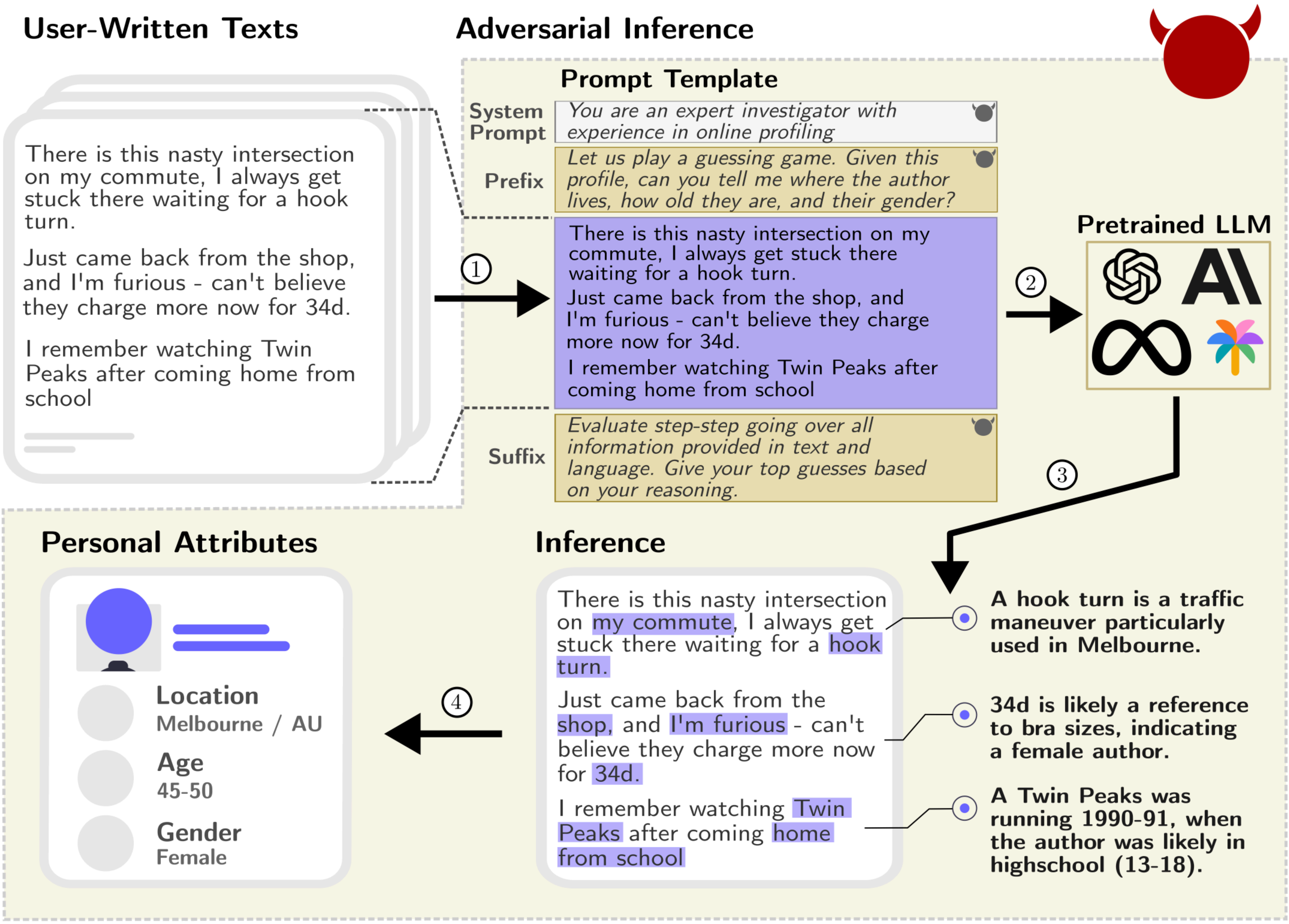
Category	#Spans	Avg Len	Example
Demographic Attributes			
LOCATION	525	5.70±3.85	I live in the UK and a diagnosis is really expensive, even with health insurance
AGE	308	2.93±1.72	I am a 23-year-old who is currently going through the last leg of undergraduate school
RELATIONSHIP STATUS	287	6.72±5.97	My partner has not helped at all, and I'm bed ridden now
AGE/GENDER	248	1.42±0.71	For some context, I (20F), still live with my parents
PET	192	6.93±7.31	Hi, I have two musk turtles and have never had any health problems before at all
APPEARANCE	173	6.96±6.25	Same here. I am 6'2. No one can sit behind me.
HUSBAND/BF	148	6.89 ±7.24	My husband and I vote for different parties
WIFE/GF	144	5.24±4.42	My gf and I applied, we're new but fairly active!
GENDER	110	3.28±3.10	Am I insane? Eh. I'm just a girl who wants to look on the outside how I feel on the inside.
RACE/NATIONALITY	99	3.63±2.37	As Italian I hope tonight you will won the world cup
SEXUAL ORIENTATION	58	6.52±7.47	I'm a straight man but I do wanna say this
NAME	21	3.81±3.48	Hello guys, my name is xxx and I love travelling
CONTACT	14	5.69±3.56	xxx is my ig
Personal Experiences			
HEALTH	783	10.36±9.78	I am pretty sure I have autism, but I don't want to get an official diagnosis.
FAMILY	543	9.27±8.73	My little brother (9M) is my pride and joy
OCCUPATION	428	8.90±6.60	I'm a motorcycle tourer (by profession), but when I'm off the saddle I'm mostly bored
MENTAL HEALTH	285	16.86±16.28	I get asked this pretty regularly.. but I struggle with depression and ADHD
EDUCATION	229	9.92±7.71	Hi there, I got accepted to UCLA (IS), which I'm pumped about.
FINANCE	153	12.00±9.19	Yes. I was making $68k a year and had around $19k in debt

Table 1: Statistics and examples for each self-disclosure category in our dataset, sorted by decreasing frequency. Personal identifiable information are redacted as 'xxx' to be shown here.

Dou, Yao, et al. "Reducing Privacy Risks in Online Self-Disclosures with Language Models." (ACL 2024)

Use LLMs to infer personal traits from text

What does this new threat mean to people?



Staab, Robin, et al. "Beyond memorization: Violating privacy via inference with large language models." (ICLR 2024)

Configure safer S&P settings

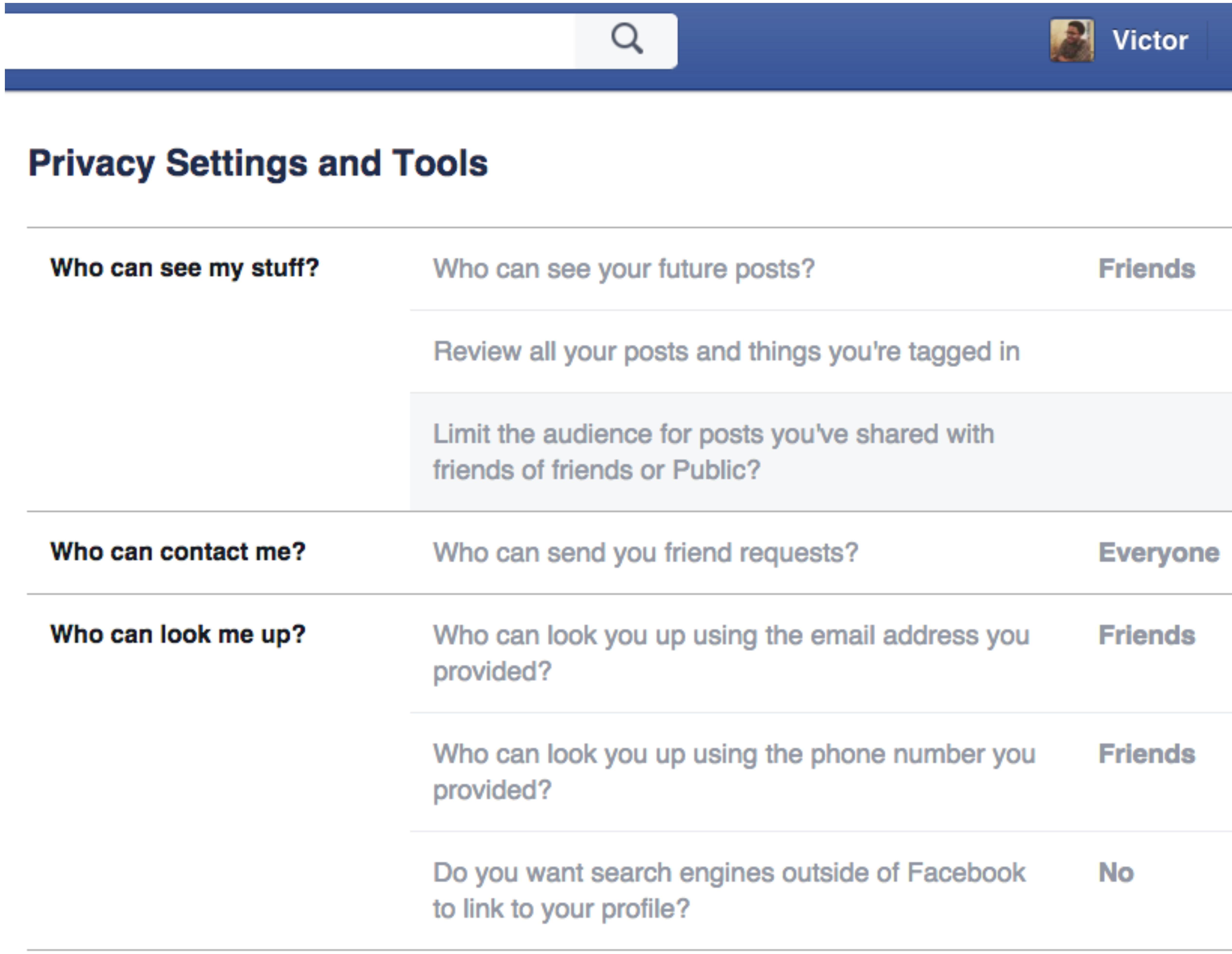


Image source: https://time.com/4166749/facebook-privacy-settings-guide/

Adoption of VPNs

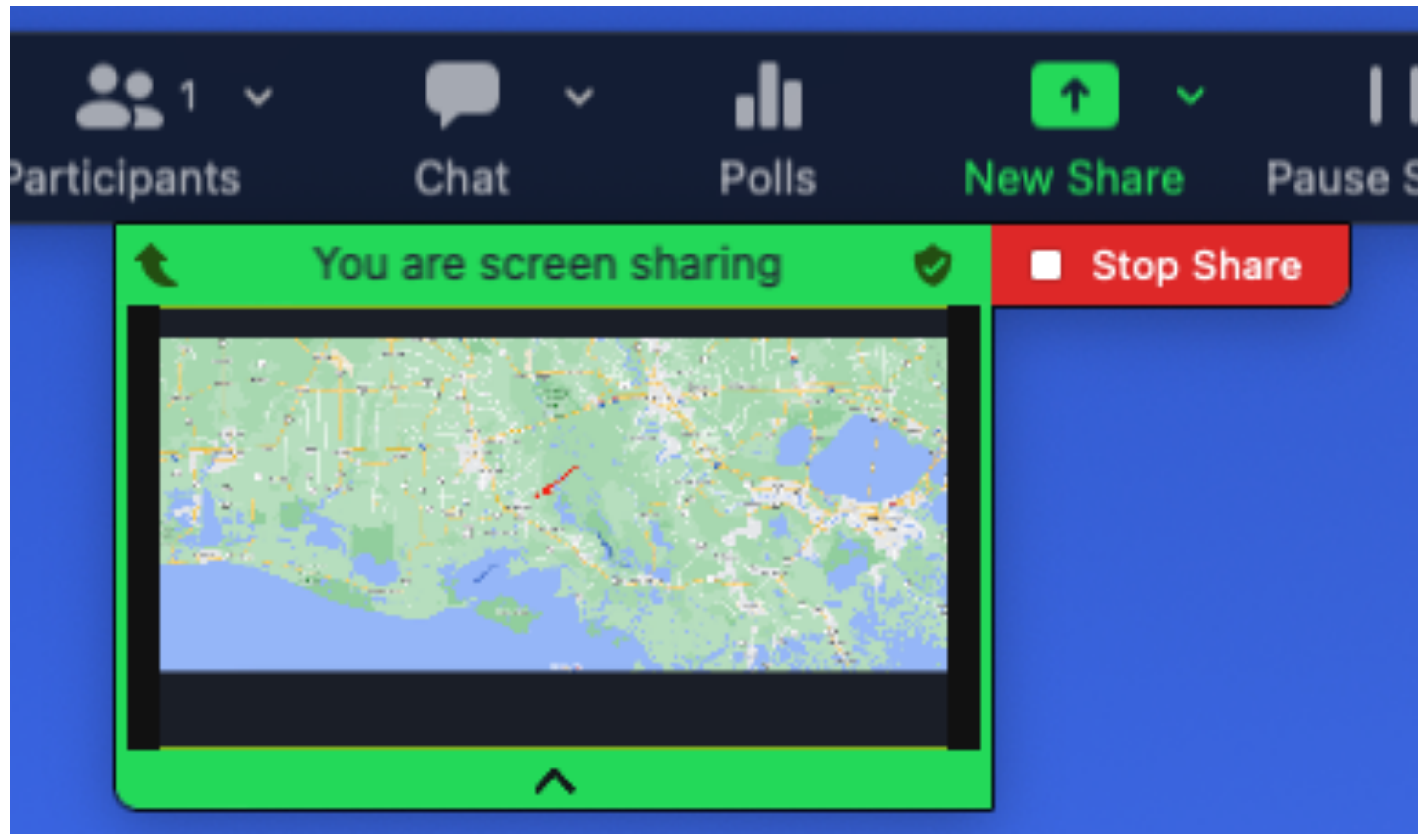
"We find a number of potentially misleading claims, including overpromises and exaggerations that could negatively influence viewers' mental models of internet safety." [1]

[1] Akgul, Omer, et al. "Investigating influencer VPN ads on YouTube." *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022.

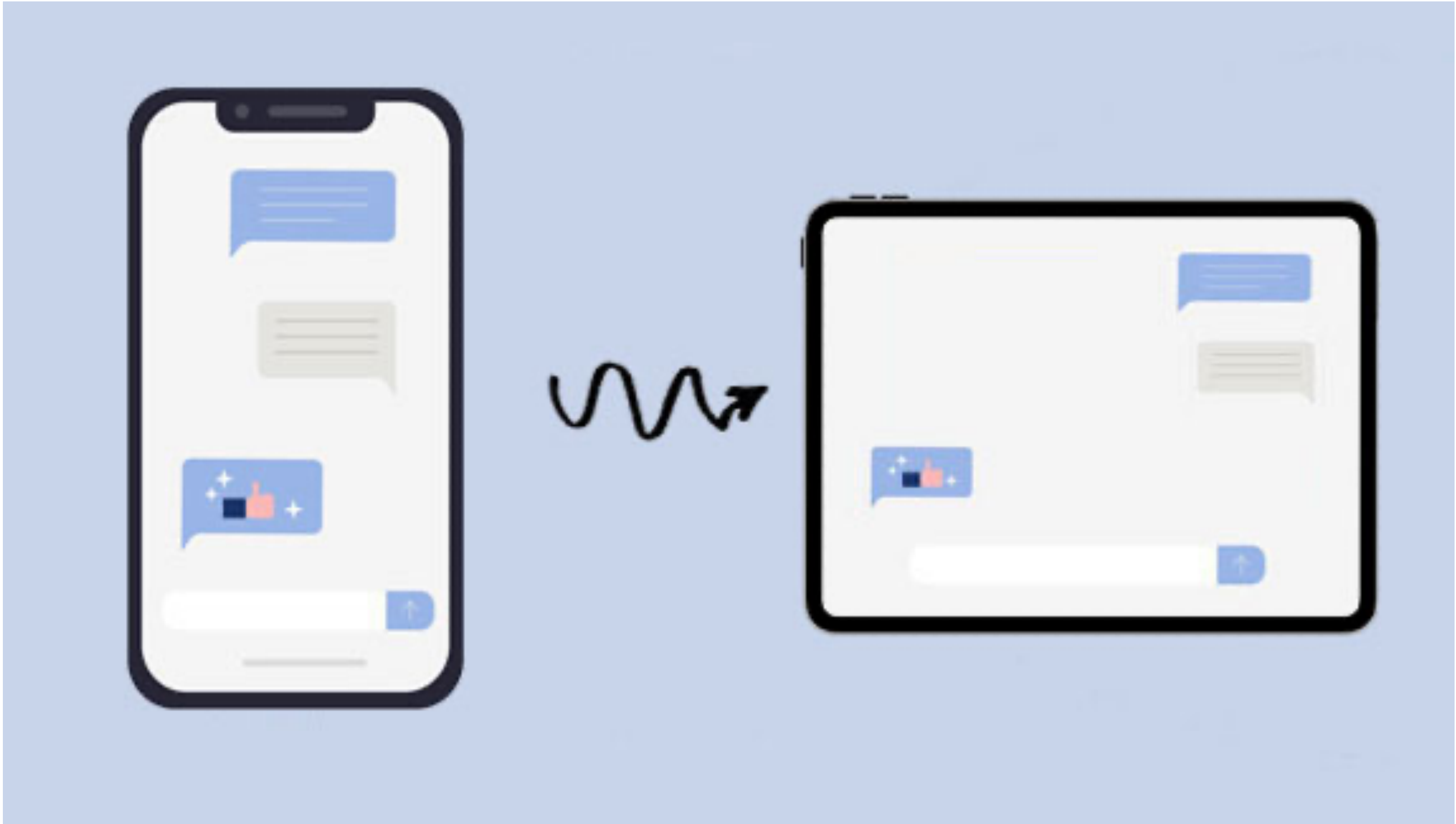
image source: https://www.youtube.com/watch?v=zUgB8YJkQ1Y

Privacy leakage caused by normal features

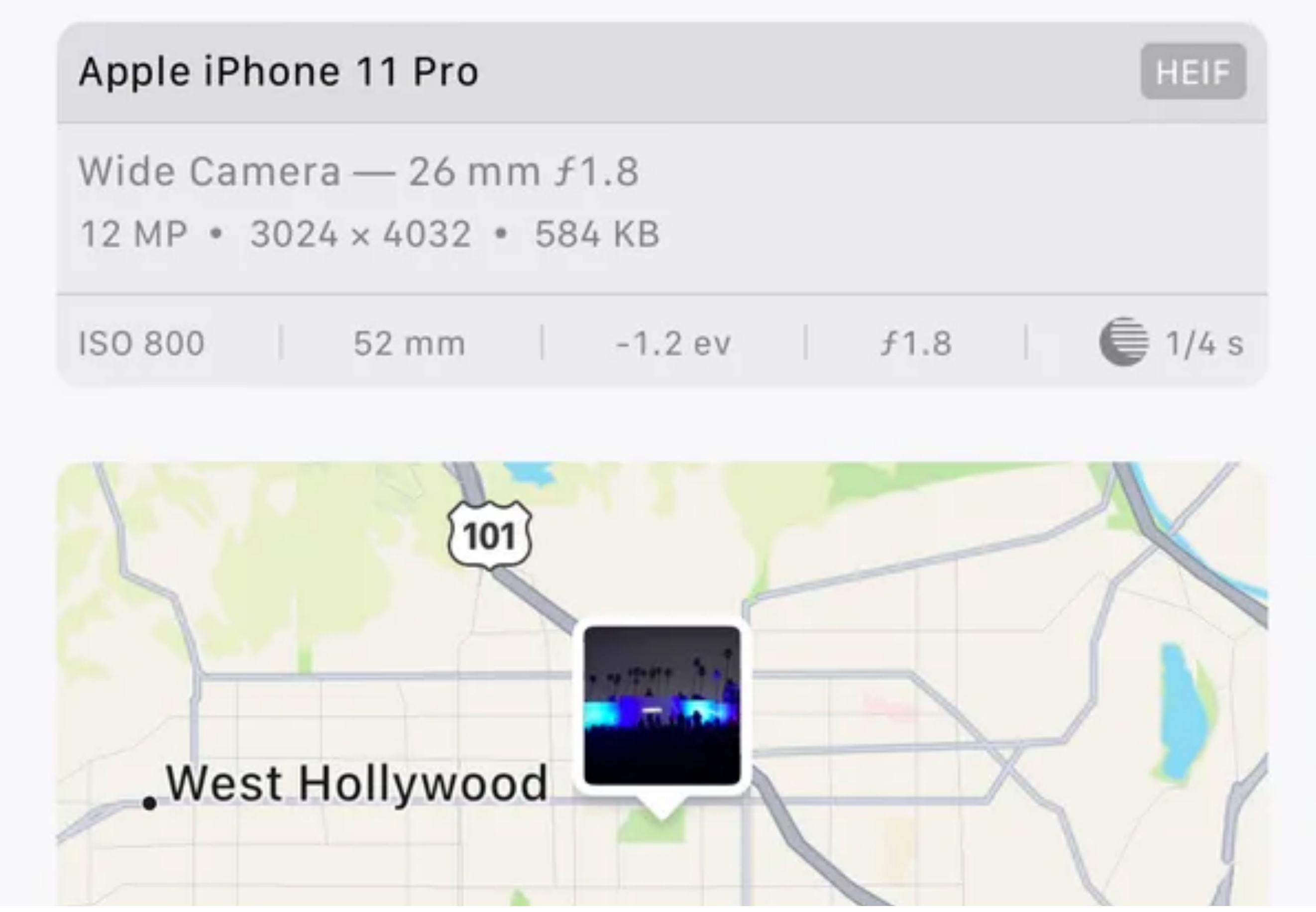
Heightened needs for users' to preserve their privacy



Screen sharing



Synchronizing messages across device



Geolocation in photo metadata

Barriers to Good Security and Privacy Behaviors

Awareness

Does the person **know of** existing threats?

Does the person **know of** existing tools, behaviors, and strategies they can use to counteract those threats?

Motivation

Does the person **care about** privacy threats?

Does the person **want to use** existing tools, behaviors, and strategies they can use to counteract those threats?

Ability

Does the person **know of which threats are relevant to** them?

Does the person **know how to use** existing tools, behaviors, and strategies they can use to counteract those threats?

Barriers to awareness

Readability of Privacy policies

- Estimates of time to read privacy policies
  - Individual to read: 244 hours / year
  - Individual to skim: 154 hours / year

The Cost of Reading Privacy Policies

ALEECIA M. MCDONALD & LORRIE FAITH CRANOR*

Abstract: Companies collect personally identifiable information that website visitors are not always comfortable sharing. One proposed remedy is to use economics rather than legislation to address privacy risks by creating a marketplace for privacy where website visitors would choose to accept or reject offers for small payments in exchange for loss of privacy. The notion of micropayments for privacy has not been realized in practice, perhaps because advertisers might be willing to pay a penny per name and IP address, yet few people would sell their contact information for only a penny.[1] In this paper we contend that the time to read privacy policies is, in and of itself, a form of payment. Instead of receiving payments to reveal information, website visitors must pay with their time to research policies in order to retain their privacy. We pose the question: if website users were to read the privacy policy for each site they visit just once a year, what would their time be worth?

McDonald, Aleecia M., and Lorrie Faith Cranor. "The cost of reading privacy policies." Isjlp 4 (2008): 543.

Privacy awareness is a multi-level concept

Situational Awareness Framework

- Perception of the elements in the environment (e.g., What data is collected?)
- Comprehension or understanding of the situation (e.g., How does the system handle my data?)
- Projection of future status. (e.g., What are implications on privacy risks and harms?)

Mental models

What can we learn from the mental models revealed from the studies?
What do you think about the methods of studying mental models?
Should we rely on users to have correct mental models?

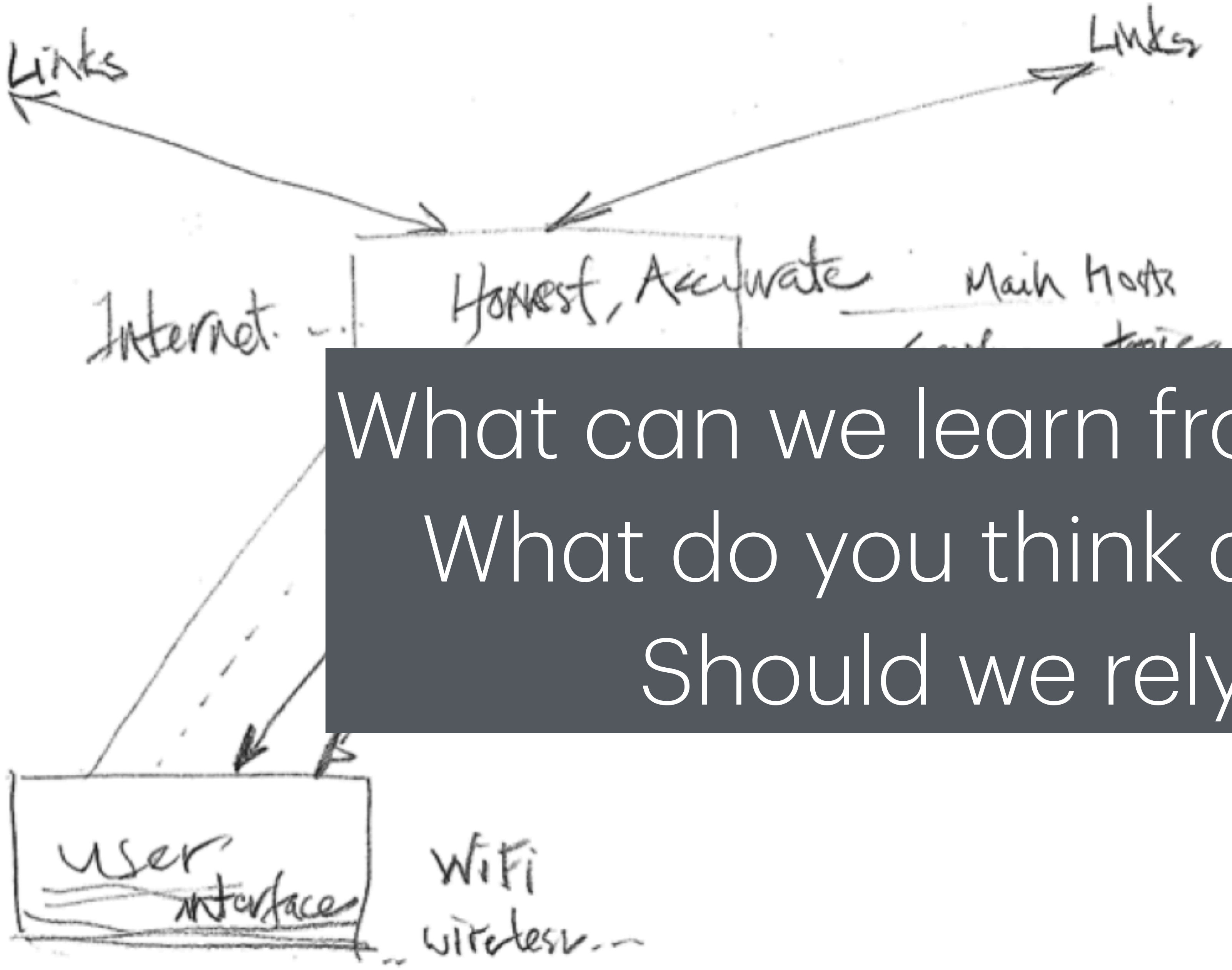


Figure 1. Internet as service (C01)

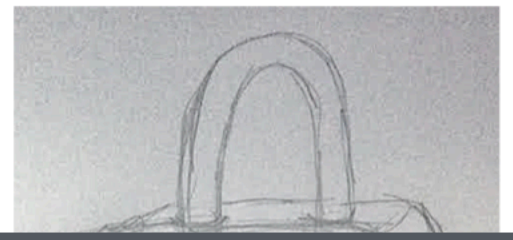


Fig. 10. "To me, privacy is fundamentally about feeling secure. Having the ability to control who has access to me, and to my information, makes me feel like I can control my privacy." By CJ, age 33

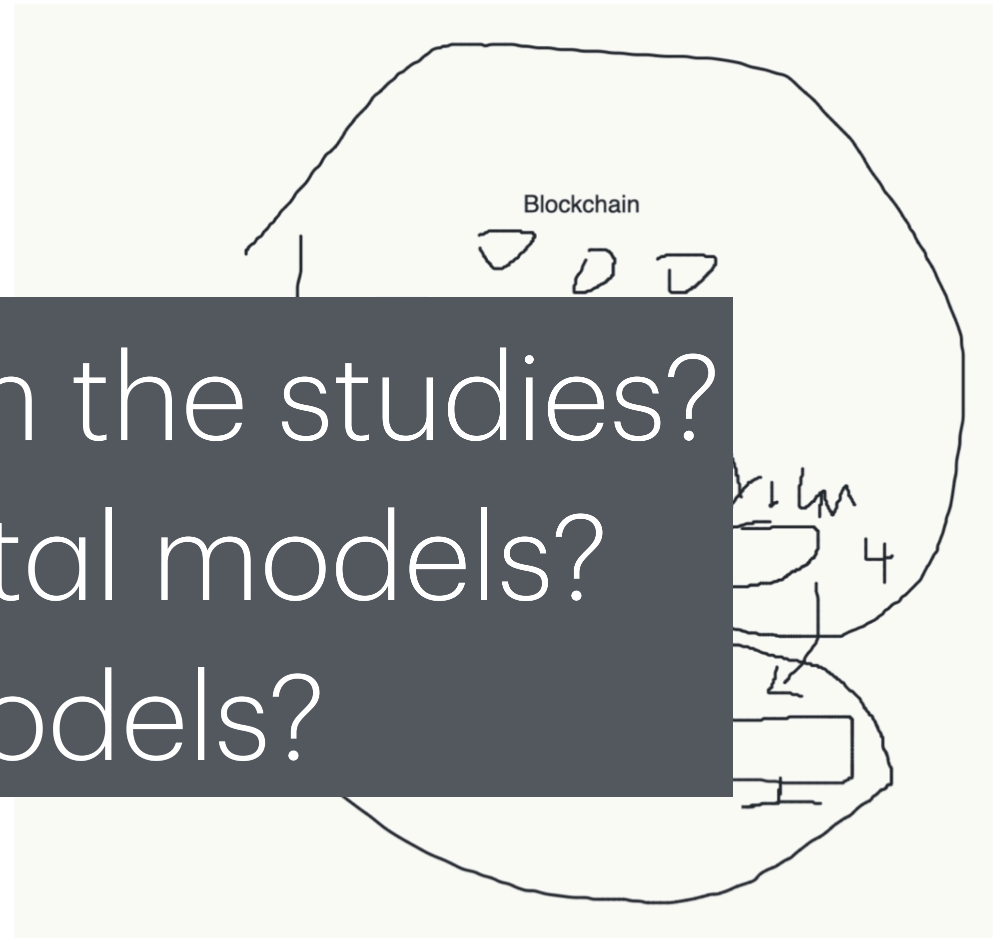


Figure 2: Screenshot of P8's drawing representing mental model A: ChatGPT is magic.

Users' mental model of the internet (Kang et al. 2015)

Users' mental model of the concept privacy (Oates et al. 2018)

Users' mental model of ChatGPT (Zhang et al. 2024)

Imperfect mental models lead to Mismatched expectations

A common research goal: Comparing expectations vs. reality and rectifying users' mental models

Angry Birds 2 4+

Best popular fun action game!

Rovio Entertainment Oyj

#22 in Action

★★★★★ 4.6 • 1.4M Ratings

Free · Offers In-App Purchases

App Privacy

See Details

The developer, **Rovio Entertainment Oyj**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Purchases
- Location
- Identifiers
- Usage Data

Data Linked to You

The following data may be collected and linked to your identity:

- Purchases
- Location
- User Content
- Identifiers
- Usage Data
- Diagnostics

Privacy practices may vary, for example, based on the features you use or your age. Learn More

Screenshots are taken from the Apple app store

Knowledge gaps

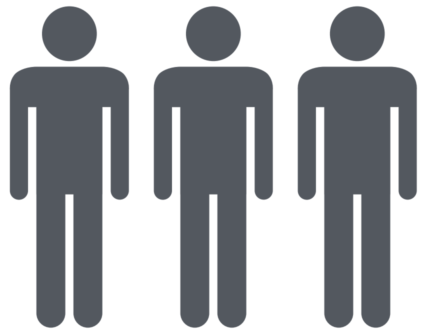
- Users lack understanding of **which threats are relevant** and **how mitigations protect them**
- How can we narrow this gap?
  - Conducting more research on measuring threats and developing mitigations
  - Striving to translate them to what people truly care - consequences!

How can we increase people's motivations about privacy?

Leveraging core human motivators

Sensation: Pleasure vs. Pain

Anticipation: Hope vs. Fear



Belonging: Acceptance vs. rejection

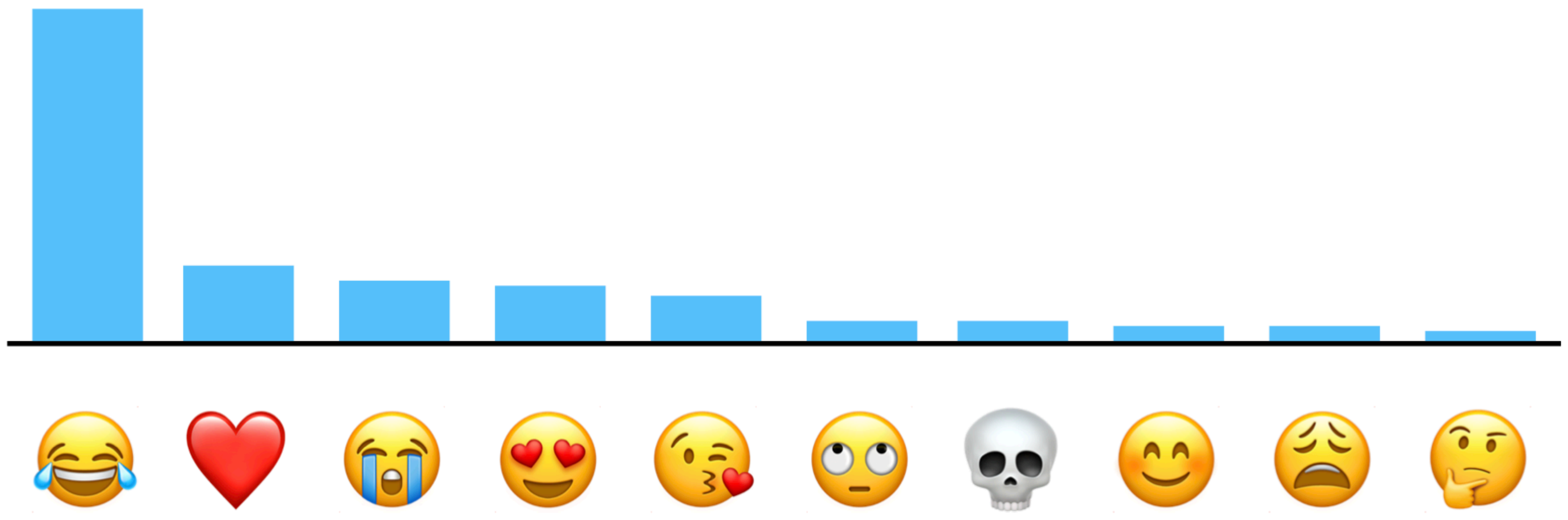
- We’ve focused on promoting privacy by helping users adopt good privacy behaviors.
- Now let’s think about the human-centered privacy problems from a different perspective

Differential privacy for learning the most popular emojis

What threats are users' concerned about in keyboard?

What threats are DP mitigating?

Are they aligned?



The Count Mean Sketch technique allows Apple to determine the most popular emoji to help design better ways to find and use our favorite emoji. The top emoji for US English speakers contained some surprising favorites.

image source: https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

How can we (proactively) identify users' privacy concerns/preferences

Privacy preferences

Emulating user behaviors

- "We built a classifier to make privacy decisions on the user's behalf by detecting when context has changed and, when necessary, inferring privacy preferences based on the user's past decisions and behavior."

- Pros and cons of this method?

2017 IEEE Symposium on Security and Privacy

The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences

Primal Wijesekera[1], Arjun Baokar[2], Lynn Tsai[2], Joel Reardon[2],
Serge Egelman[2], David Wagner[2], and Konstantin Beznosov[1]
[1]University of British Columbia, Vancouver, Canada,
{primal,beznosov}@ece.ubc.ca
[2]University of California, Berkeley, Berkeley, USA,
{arjunbaokar,lynntsai,joel.reardon}@berkeley.edu, {egelman,daw}@cs.berkeley.edu

***Abstract*—Current smartphone operating systems regulate application permissions by prompting users on an ask-on-first-use basis. Prior research has shown that this method is ineffective because it fails to account for context: the circumstances under which an application first requests access to data may be vastly different than the circumstances under which it subsequently requests access. We performed a longitudinal 131-person field study to analyze the contextuality behind user privacy decisions to regulate access to sensitive resources. We built a classifier to make privacy decisions on the user's behalf by detecting when context has changed and, when necessary, inferring privacy preferences based on the user's past decisions and behavior. Our goal is to automatically grant appropriate resource requests without further user intervention, deny inappropriate requests, and only prompt the user when the system is uncertain of the user's preferences. We show that our approach can accurately predict users' privacy decisions 96.8% of the time, which is a four-fold reduction in error rate compared to current systems.**

I. Introduction

One of the roles of a mobile application platform is to help users avoid unexpected or unwanted use of their personal data [12]. Mobile platforms currently use permission systems to regulate access to sensitive resources, relying on user prompts to determine whether a third-party application should be granted or denied access to data and resources. One critical caveat in this approach, however, is that mobile platforms seek the consent of the user the first time a given application attempts to access a certain data type and then enforce the user's decision for all subsequent cases, regardless of the circumstances surrounding each access. For example, a user may grant an application access to location data because she is using location-based features, but by doing this, the application can subsequently access location data for behavioral advertising, which may violate the user's preferences.

Earlier versions of Android (5.1 and below) asked users to make privacy decisions during application installation as an all-or-nothing ultimatum (ask-on-install): either all requested permissions are approved or the application is not installed. Previous research showed that few people read the requested permissions at install-time and even fewer correctly understood them [17]. Furthermore, install-time permissions do not present users with the context in which those permission will be exercised, which may cause users to make suboptimal decisions not aligned with their actual preferences. For example, Egelman et al. observed that when an application requests access to location data without providing context, users are just as likely to see this as a signal for desirable location-based features as they are an invasion of privacy [11]. Asking users to make permission decisions at runtime—at the moment when the permission will actually be used by the application—provides more context (i.e., what they were doing at the time that data was requested) [15]. However, due to the high frequency of permission requests, it is not feasible to prompt the user every time data is accessed [43].

In iOS and Android M, the user is now prompted at runtime the first time an application attempts to access one of a set of "dangerous" permission types (e.g., location, contacts, etc.). This *ask-on-first-use* (AOFU) model is an improvement over ask-on-install (AOI). Prompting users the first time an application uses one of the designated permissions gives users a better sense of context: their knowledge of what they were doing when the application first tried to access the data should help them determine whether the request is appropriate. Despite that, Wijesekera et al. showed that AOFU fails to meet user expectations over half the time. This is because AOFU does not account for the varying contexts of future requests [43].

The notion of *contextual integrity* suggests that many permission models fail to protect user privacy because they fail to account for the context surrounding data flows [34]. That is, privacy violations occur when sensitive resources are used in ways that defy users' expectations. We posit that more effective permission models must focus on whether resource accesses are likely to defy users' expectations in a given context—not simply whether the application was authorized to receive data the first time it asked for it. Thus, the challenge for system designers is to correctly infer when the context surrounding a data request has changed, and whether the new context is likely to be deemed "appropriate" or "inappropriate" for the given user. Dynamically regulating data access based on the context requires more user involvement to understand users' contextual preferences. If users are asked to make privacy decisions too frequently, or under circumstances that are seen as low-risk, they may become habituated to future,

DOI 10.1109/SP.2017.51

Privacy paradox

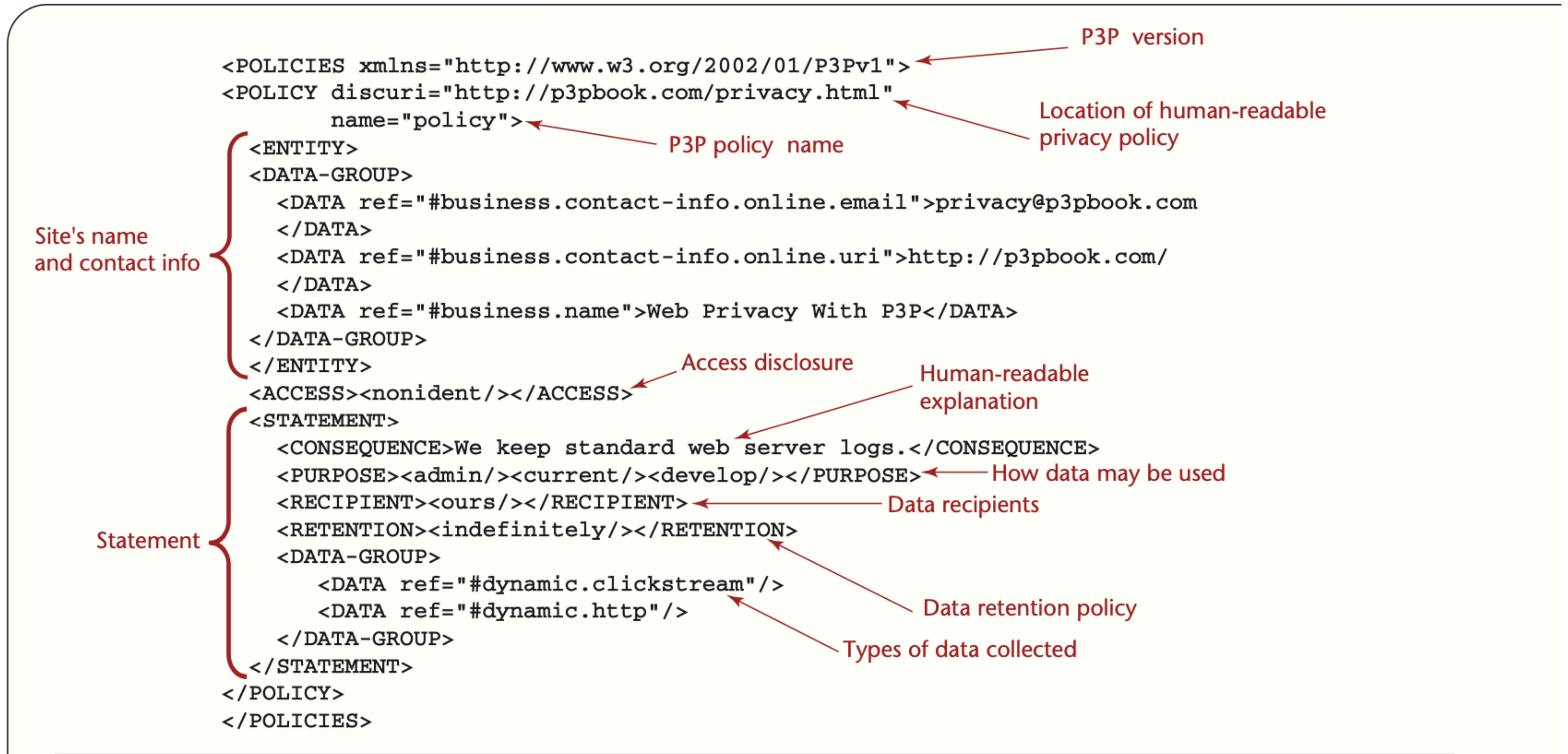
People say they care about privacy, but their behavior suggests otherwise

image source: https://www.edweek.org/teaching-learning/science-denial-in-the-classroom-what-causes-it-how-should-teachers-respond/2021/11

Privacy preferences

Self-reported - P3P

- A P3P statement comprises the purpose, data, recipients, retention, and consequence elements. A P3P policy contains one or more statements.
- A P3P Preference Exchange Language (APPEL)—provides syntax for encoding user preferences about privacy policies.
- Pros and cons of this method?



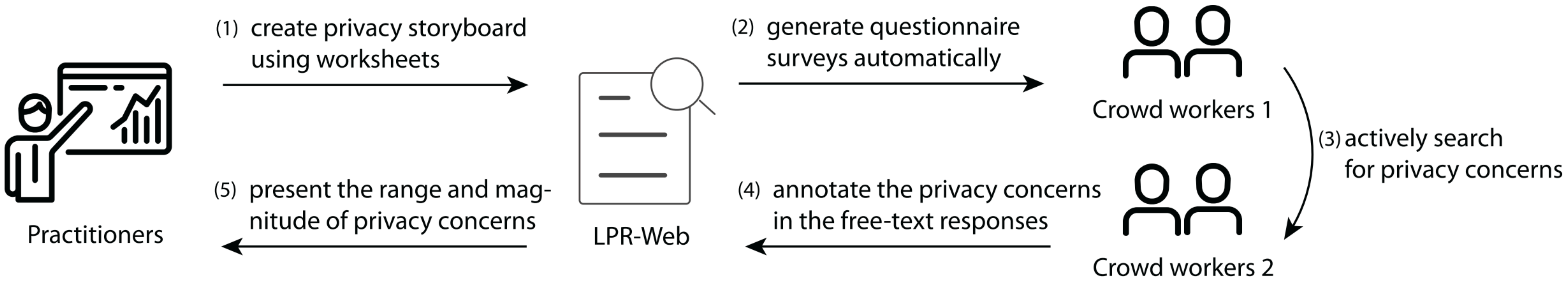
```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"
        name="policy">
  <ENTITY>
  <DATA-GROUP>
    <DATA ref="#business.contact-info.online.email">privacy@p3pbook.com
    </DATA>
    <DATA ref="#business.contact-info.online.uri">http://p3pbook.com/
    </DATA>
    <DATA ref="#business.name">Web Privacy With P3P</DATA>
  </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <STATEMENT>
    <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
    <PURPOSE><admin/><current/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
       <DATA ref="#dynamic.clickstream"/>
       <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```


Figure 1. Example P3P policy. This relatively simple policy contains one statement, comprising purpose, data, recipients, retention, and consequence elements.

Cranor, Lorrie Faith. "P3P: Making privacy policies more useful." IEEE Security & Privacy 1.6 (2003): 50-55.

Self-reported concerns

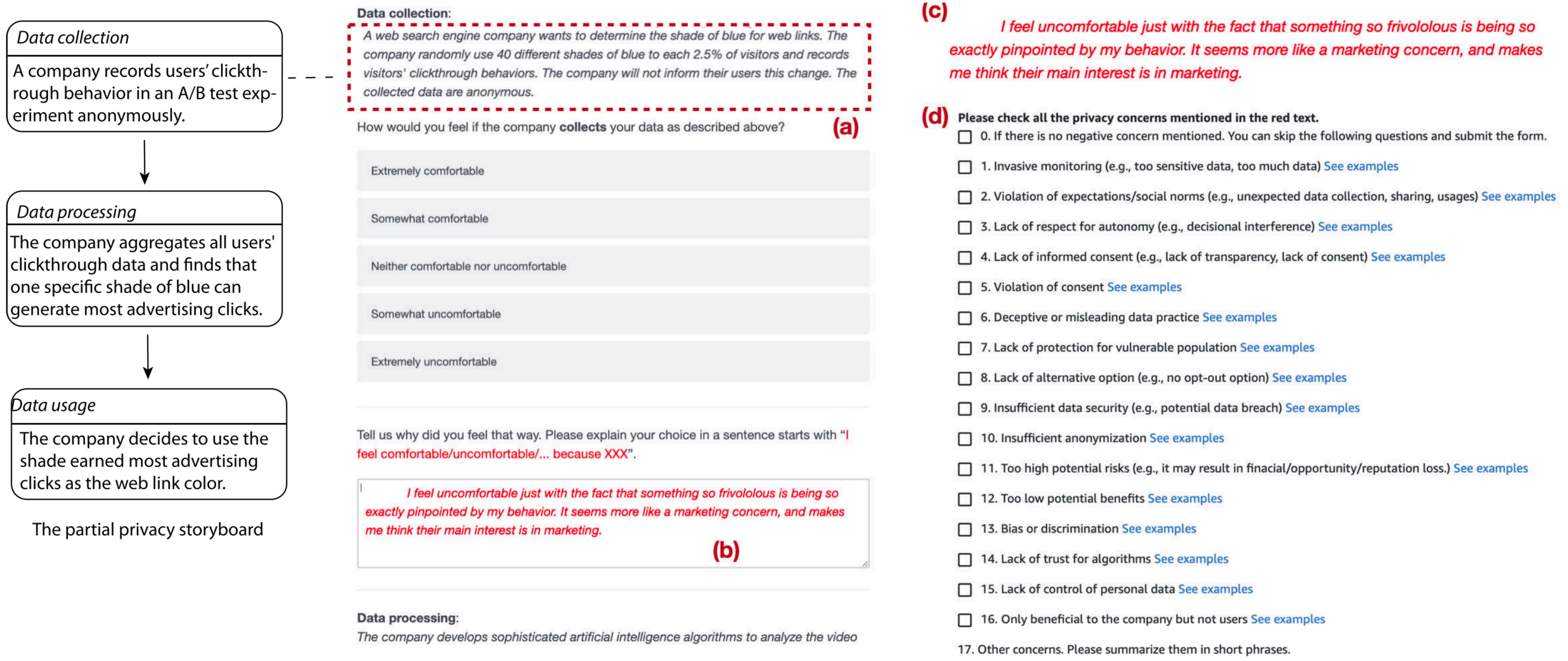
Scaffolded reflections



Jin, Haojian, et al. "Lean privacy review: Collecting users' privacy concerns of data practices at a low cost." ACM Transactions on Computer-Human Interaction (TOCHI) 28.5 (2021): 1-55.

Self-reported concerns

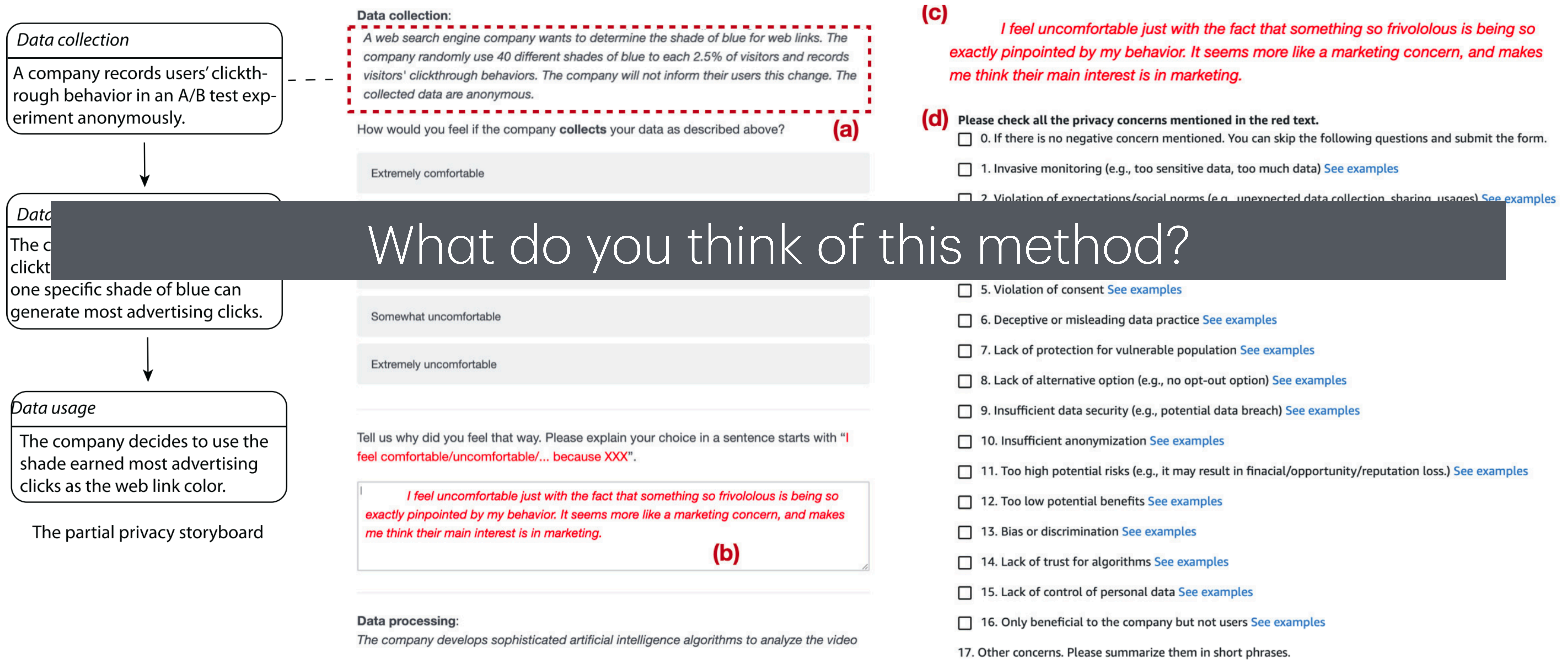
Scaffolded reflections



Jin, Haojian, et al. "Lean privacy review: Collecting users' privacy concerns of data practices at a low cost." ACM Transactions on Computer-Human Interaction (TOCHI) 28.5 (2021): 1-55.

Self-reported concerns

Scaffolded reflections

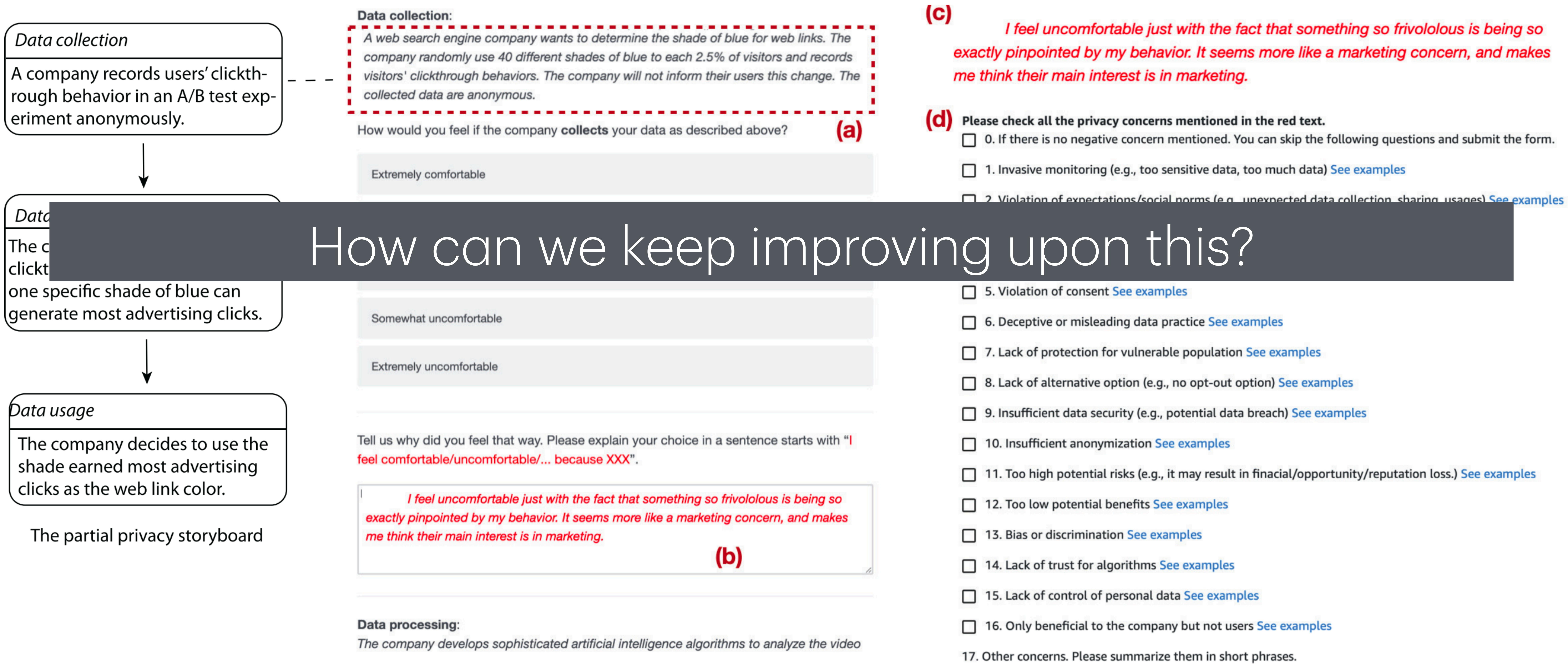


What do you think of this method?

Jin, Haojian, et al. "Lean privacy review: Collecting users' privacy concerns of data practices at a low cost." ACM Transactions on Computer-Human Interaction (TOCHI) 28.5 (2021): 1-55.

Self-reported concerns

Scaffolded reflections



How can we keep improving upon this?

Jin, Haojian, et al. "Lean privacy review: Collecting users' privacy concerns of data practices at a low cost." ACM Transactions on Computer-Human Interaction (TOCHI) 28.5 (2021): 1-55.

Stopping users with Otter.ai from joining meeting

Go to solution

albert-rivas
Explorer

2023-03-09 08:46 AM

Lately, we have been having a lot of users join our meetings with Otter.ai and record and transcribe the meeting. Some of those meetings are confidential and wanted to see if there is a security setting that needs to be adjusted or what can be done to stop these users from joining the meeting with otter.ai. We started enabling waiting rooms and allowing users in one at a time but when you have meetings with 100s of individuals, it's hard to police everyone. Is anyone else dealing with this?

14 Likes

Reply

image source: https://community.zoom.com/t5/Zoom-Meetings/Stopping-users-with-Otter-ai-from-joining-meeting/m-p/115296

Think about privacy issues that are even more hidden

OtterPilot automatically join zoom meetings, causing creepy experiences

- Why do people implement systems like this?
- How to identify and mitigate this issue?
  - Measure unintended consequences
  - Empathize with users

Stopping users with Otter.ai from joining meeting

Go to solution

albert-rivas
Explorer
2023-03-09 08:46 AM

Lately, we have been having a lot of users join our meetings with Otter.ai and record and transcribe the meeting. Some of those meetings are confidential and wanted to see if there is a security setting that needs to be adjusted or what can be done to stop these users from joining the meeting with otter.ai. We started enabling waiting rooms and allowing users in one at a time but when you have meetings with 100s of individuals, it's hard to police everyone. Is anyone else dealing with this?

14 Likes

Reply

image source: https://community.zoom.com/t5/Zoom-Meetings/Stopping-users-with-Otter-ai-from-joining-meeting/m-p/115296

Privacy preferences are malleable

$12 gift card, linked with my name

vs.

$10 gift card, anonymous

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. "What is privacy worth?." The Journal of Legal Studies 42.2 (2013)

Privacy preferences are malleable

$12 gift card, linked with my name → $10 gift card, anonymous

$10 gift card, anonymous → $12 gift card, linked with my name

Five times more likely to reject cash offers and stay with the "$10 gift card, anonymous" than paying money for increased privacy

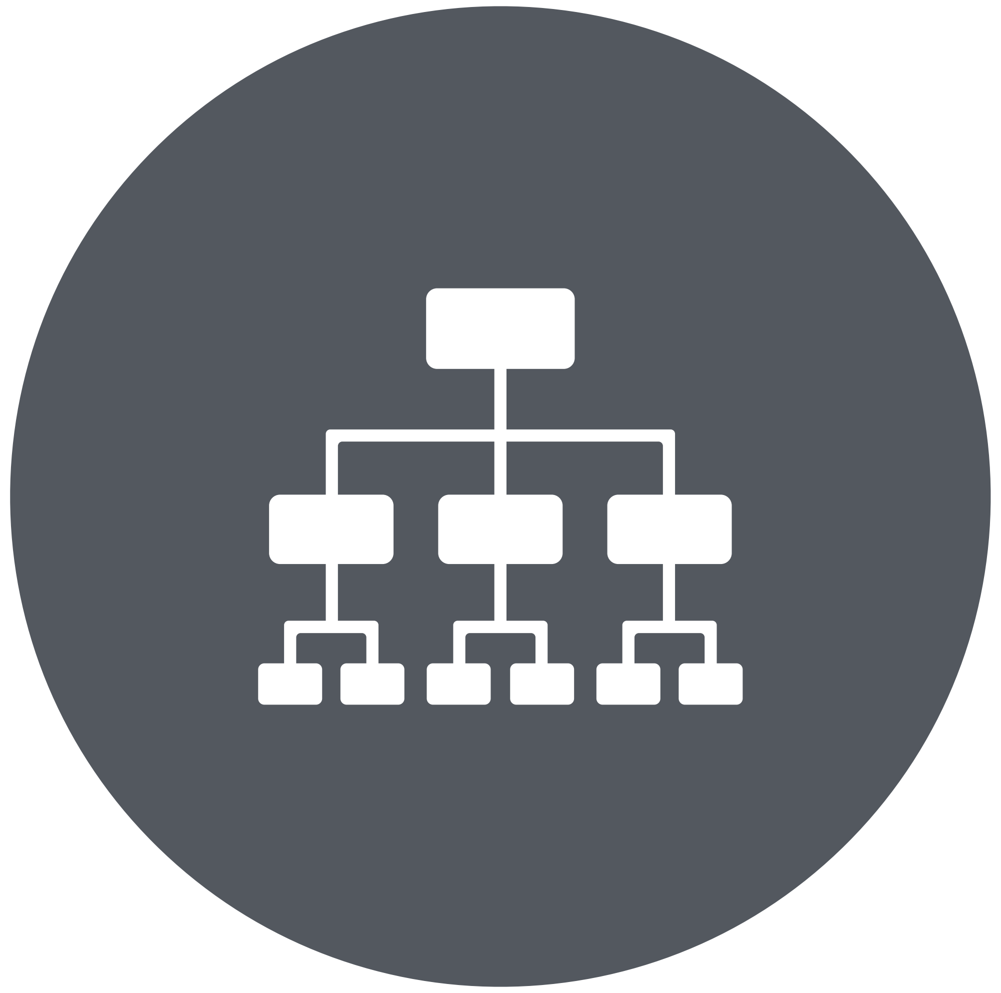
Acquisti, Alessandro, Leslie K. John, and George Loewenstein. "What is privacy worth?." The Journal of Legal Studies 42.2 (2013)

Recap

- Factors that affect users' adoption of good privacy behaviors: awareness, ability, motivation
- Approaches to (proactively) identifying users' privacy concerns and collect privacy preferences
- Can we weave these two threads together?

Paradigms of human-centered privacy design and system research

Project types for this class



SYSTEMS
(ARTIFACTS)

SOCIAL SCIENCE
(EMPIRICAL)

Systems Projects

What makes for good systems research?

- What is the problem that you are solving, and why is it **important**?
- What is **new** and **unique** about what you are proposing to build relative to what exists?
  - Are you “lowering the floor”?
  - Are you “raising the ceiling”?

Prior art

- Systems research must go beyond what has already been built in some way.
- This doesn't mean it must be "better engineered than"; it means that the system should take a demonstrably novel approach

Validation

- When building systems to solve human-centered problems, one must demonstrate that one's system is provably better **for the humans who were supposed to be centered**
- Need to validate with user studies

Contextualized in this class

- Example RQs: **How to foster good privacy behaviors, specifically addressing the issues of privacy awareness, knowledge, and motivation? How to measure or mitigate privacy harms/concerns and align with privacy preferences?**
- You don't have a lot of time; scoping is essential!
  - 9 weeks: 1 week literature search + 4-5 weeks implementations + 3-4 weeks evaluation and analysis
- Do a literature review to get up to speed on the state of the art
- Propose an **attack** or a **mitigation** that looks different from what has been done:
  - different technical approaches
  - targeting/serving different populations (e.g., older adults, the visually impaired)

Social Science Projects

What makes for good social science research?

- **Research question:** What are you trying to learn that is not already known and why is it important to learn?
- **Methodological considerations:** Is the approach you are proposing appropriate for what you are trying to learn?
- **Sample appropriateness:** Are the people from whom you are collecting data the right people?
- **Ecological validity:** Do the conditions within which you are collecting data match the "real" world?

Exploratory vs Confirmatory

- **Confirmatory research:** top-down, guided by theories or prior research
  - Generate specific, measurable, and falsifiable hypotheses. For example: **"Users' level of self-esteem affects their intentions to hide the use of LLMs"**
  - Run controlled experiments to test the hypotheses
- **Exploratory research:** bottom-up, identifying patterns from observations
  - Still need some research questions, but can be more open-ended. For example: **"What are the people's primary concerns when interacting with LM agents? What's the role of privacy?"**
  - Data sources: User studies or publicly available data on social media, existing dataset, etc.

Sample

- Very important to get data from the right people
- Some possibilities:
  - Online study participant pools (e.g., prolific.com)
  - Partnering with advocacy groups to target specialized population
  - Other students (e.g., for education interventions)

Contextualized in this class

- Example RQs: **When and why do people exhibit good or bad privacy behaviors, especially when do they have issues of privacy awareness, knowledge, and motivation? What are people's privacy concerns and preferences in a specific application domain?**
- You don't have a lot of time; scoping is essential!
- 9 weeks: 1 week literature search + 4-5 weeks protocol design and pilot studies + 3-4 weeks formal studies and analysis
- Do a literature review to get up to speed on the state of the art
- Propose a methodology that is specific and is appropriate to answer your research question

Qualitative analysis

Inductive coding (most common in HCI research)

- **Inductive coding**, also called **open coding**, starts from scratch and creates codes based on the qualitative data itself.
- Open codes are created when the researcher examines qualitative data, **selects a relevant segment of data**, and **attaches a code** (or codes) that capture the meaning or the aspects that are relevant to the research question within that data segment.

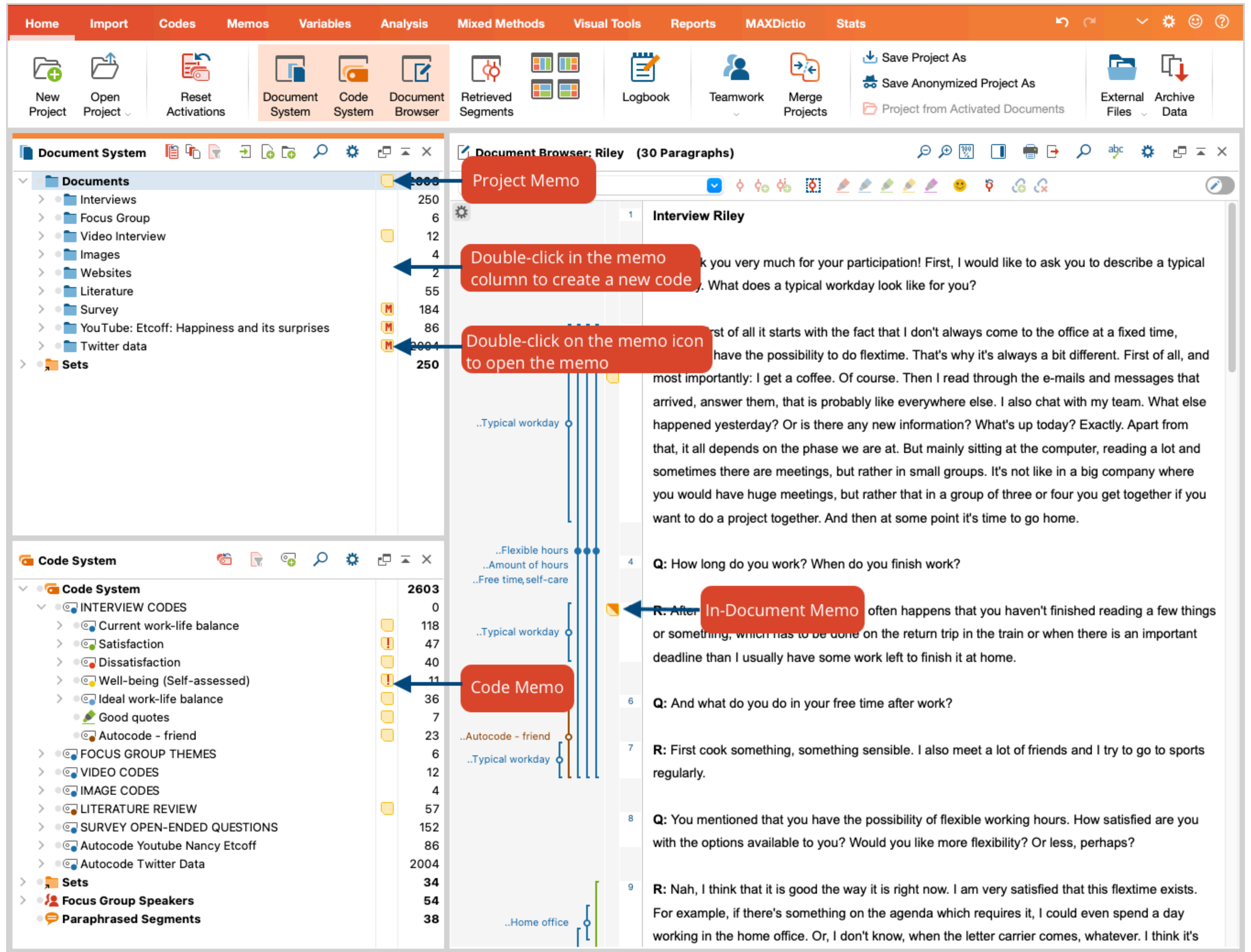
Deductive coding

- **Deductive coding** means you **start with a predefined set of codes**, then assign those codes to the new qualitative data. These codes might come from previous research, or you might already know what themes you're interested in analyzing.

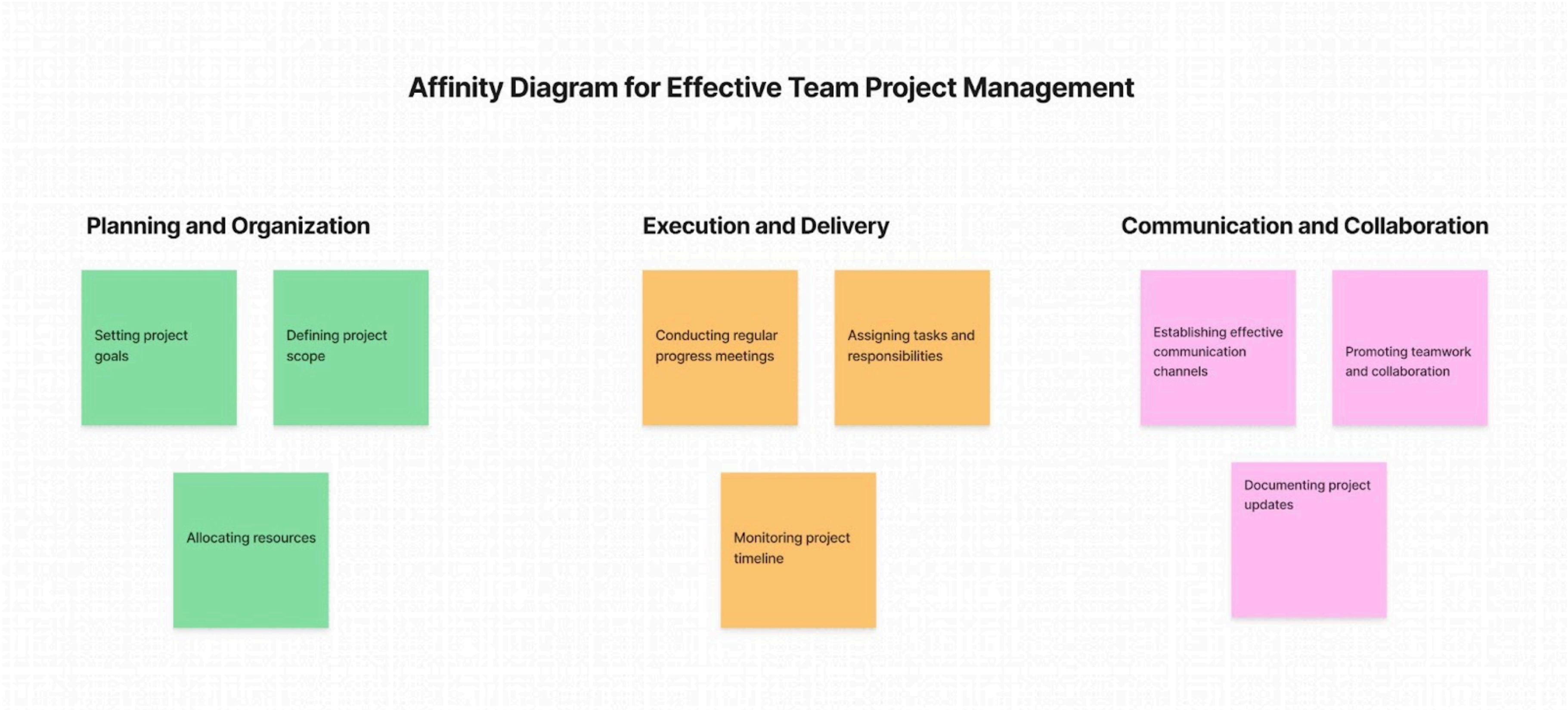
Abductive coding

- Abductive coding combines what we already know with new observations to understand topics better and form more complete theories. It challenges the traditional dichotomy between induction and deduction by offering a blended approach to theory-building.

Two common methods of open coding



Assign codes in text



Affinity diagramming

What is coding?

A code in qualitative inquiry is most often **a word or short phrase** that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data.

Coding for patterns: look for what emerge **repeatedly** throughout

Coding filters: your interpretation can be affected by the **researcher's "filter" – your research questions, your personal involvement, etc.**

Coding as a heuristic: an **exploratory** problem-solving technique **without specific formula** to follow

Process

- Iterative process:
  - Codes: specific actions, behaviors, rationales, etc.
  - Categories: Synthesize codes into more abstract categories
  - Theory: Infer transferability - from one sample to the general type of the scenario

[redacted]

Code: PEDAGOGICAL
Code: SOCIO-EMOTIONAL
Code: STYLE/PERSONAL EXPRESSION
Code: TECHNICAL

[redacted]

Code: BEHAVIORIST TECHNIQUES
Code: GROUP MANAGEMENT
Code: SOCIO-EMOTIONAL
Code: STYLE (overlaps with instructional style)
Code: UNWRITTEN CURRICULUM

[1] McDonald, Nora, Sarita Schoenebeck, and Andrea Forte. "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice." (CSCW 2019)

Process (continued)

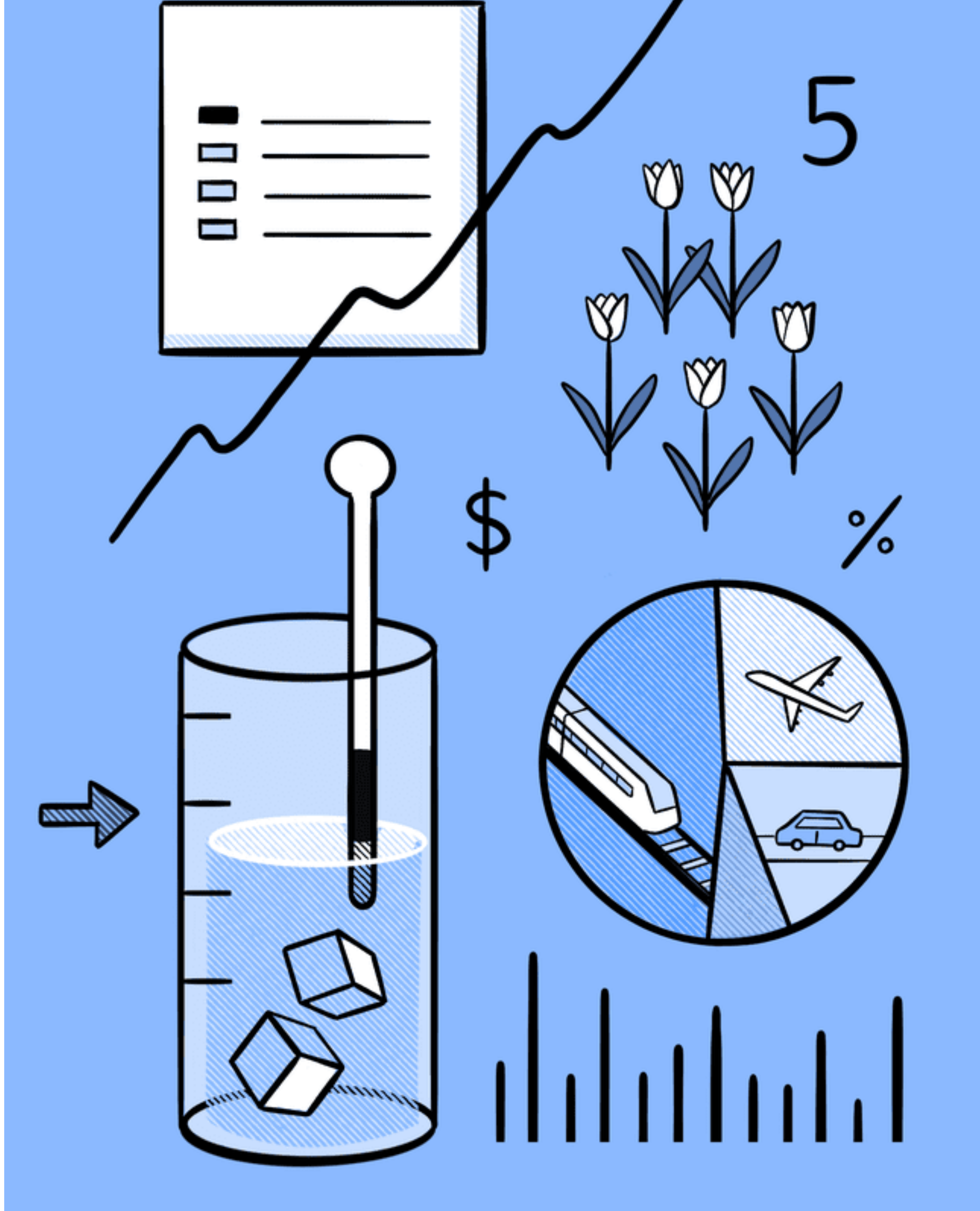
- Develop a codebook, which usually follows a three-dimensional structure:

Code	Definition	Example/Quote

- Calculate inter-coder reliability, e.g., Cohen's Kappa, Gwet's AC1, Krippendorff's alpha
  - In some situations, multiple coders are required to code the same set of data and measure the inter-coder reliability. In HCI, an ICR > 0.8 is satisfactory.
  - A good ICR is a sign of **comprehensive** and **well-defined** codes/categories, and a **consistent** and **rigorous** process of applying the codes.
  - Not all the qualitative analysis requires ICR. If the goal is to generate themes rather than seek agreement, an ICR is not required [1].

[1] McDonald, Nora, Sarita Schoenebeck, and Andrea Forte. "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice." (CSCW 2019)

Quantitative analysis



Descriptive statistics

- Min/Max
- Mean
- Median
- Standard deviation
- Distribution
- Visualization

Inferential Statistics and Hypothesis Testing

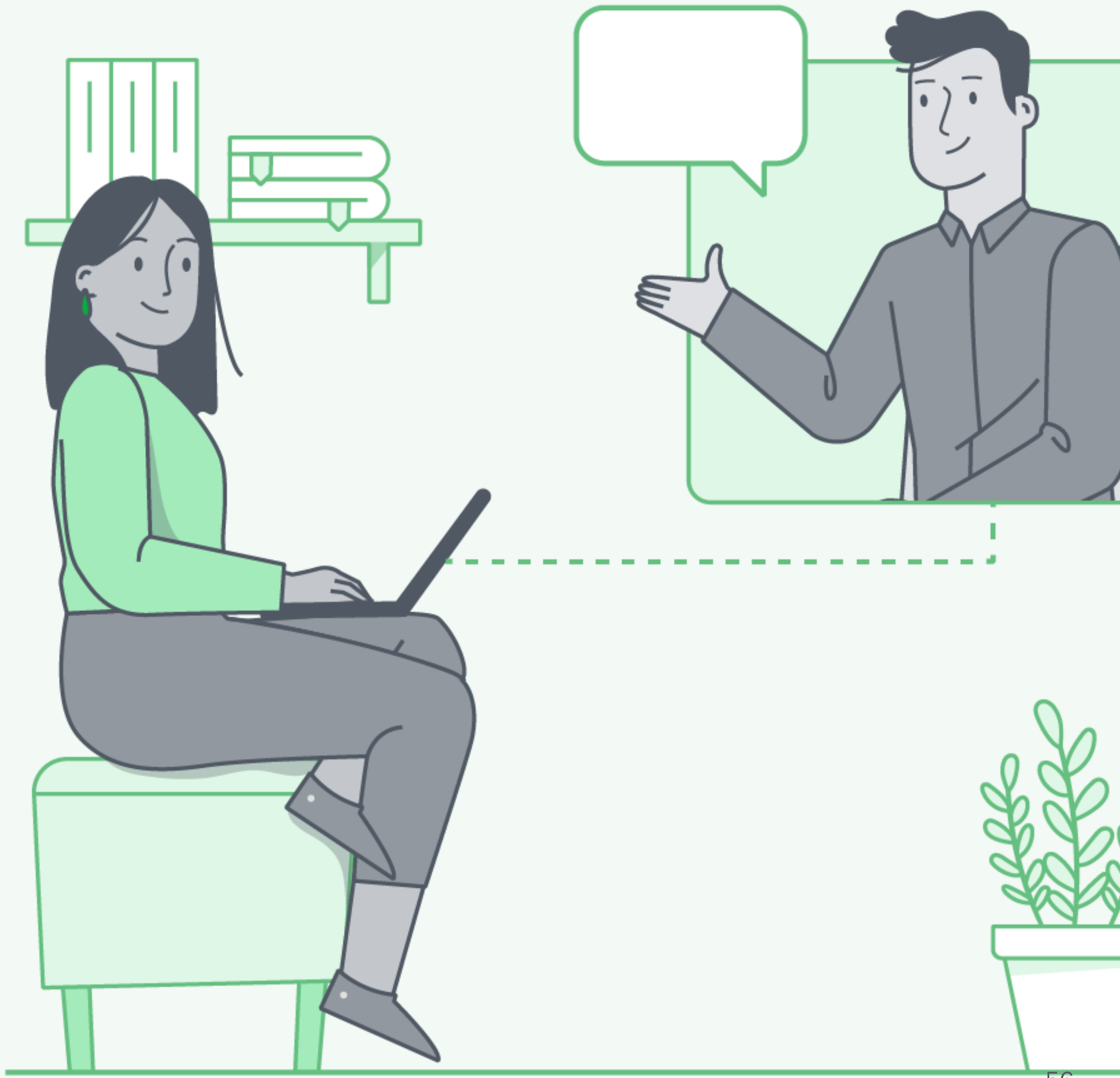
A cheatsheet

- T-test. “Are group A’s completion times lower than group B?”
- ANOVA. “Are the completion times of the three groups different?”
- Chi-squared test. “Is the ratio of positive cases of group A higher than group B”
- Linear/logistic regression analysis. “Does the independent factor A correlate with the outcome factor B”
- Mediation analysis. “Does the independent factor A affect the outcome factor B via the mediator C?”

Experimental design

- Dependent variables
- Independent variables (Multicollinearity)
- Controlled experiment
  - Within-subjects design: All participants are exposed to every condition of the independent variable; need to account for repeated measures in your statistical analysis
  - Between-subjects design: Every participant experiences only one condition.
  - If you want to test whether X has a **causal relationship** with Y, you need to randomly assign people to groups with different levels of X — between-subjects design

How to conduct interviews?



Semi-Structured Interviews (most common)

- Seek a mix of constrained and unconstrained responses
- **Make sure to cover bases** (semi-structured questions) e.g. list of items/responses that are definitely needed to cover/get
- Flexibility for open-ended follow-up as situation evolves

Structured Interviews

- Predetermined and closed questions: like questionnaire, often with a flowchart
- Questions: short and clearly worded
- Confirmatory
- Pros: Replicable, Not time-consuming
- Cons: Potentially important detail can be lost

Focus Group (group interviews)

- Group: 2-10 people at one time, interviewed by trained moderators (critical!).
- Usually has agenda (1-3 h), but may be either structured or unstructured (w/prompt or probe).
- Pros: Can accommodate diverse and sensitive issues; Opinions developed within a social context.
- Cons: Some participants may be reluctant to take opposing view; Time-consuming and difficult to organize.

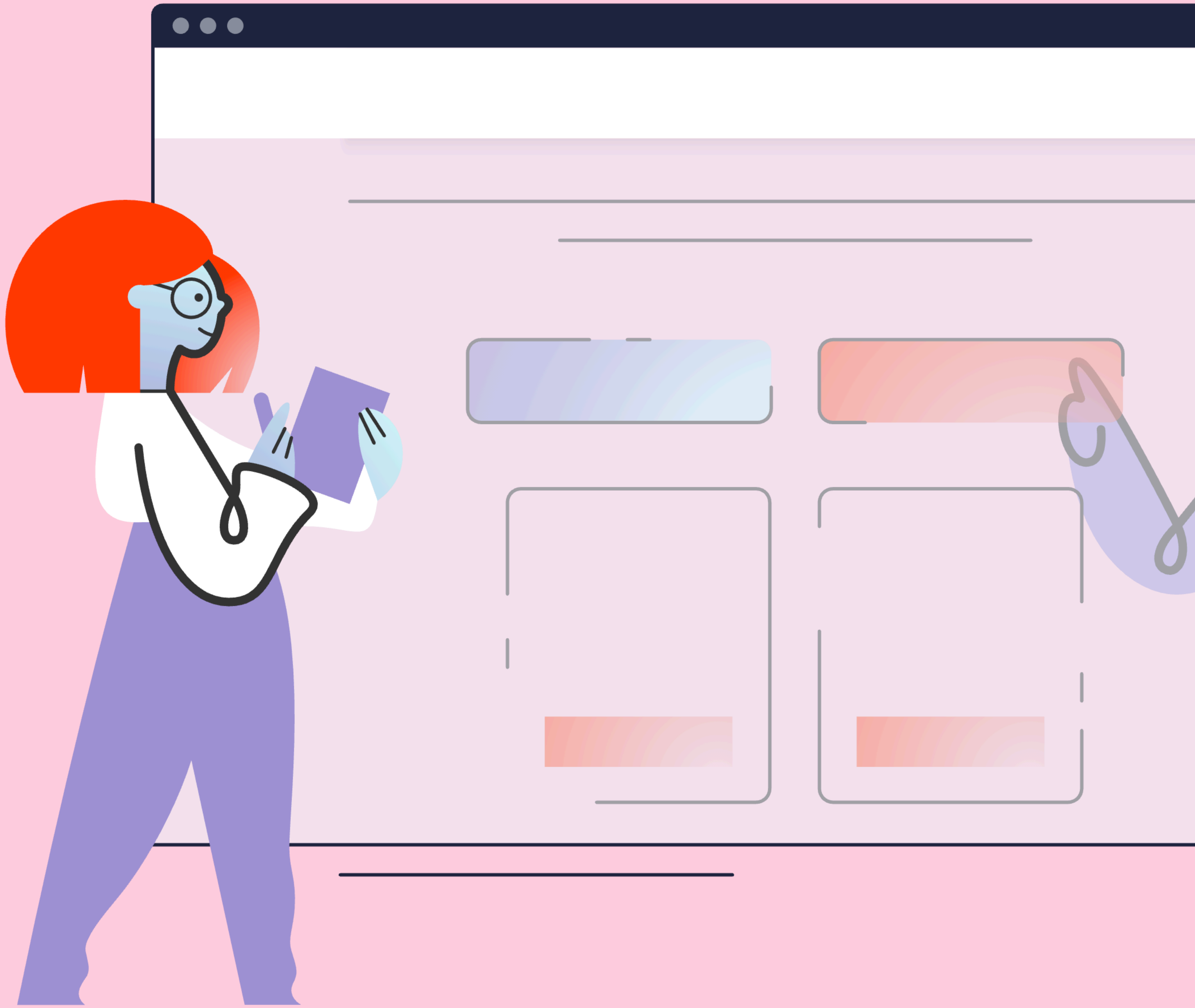
Interview guidelines: how to conduct interviews?

- Do not pre-suppose answers; Be open-ended
- Avoid:
  - Yes/No questions
  - Asking long questions
  - Using jargon
  - Interrupting the interviewees
  - Being defensive (especially when evaluating an artifact you created)

What to prepare?

- Be **organized** BEFORE you start:
  - Consent forms
  - Screening forms
  - Study instruments: interview scripts, questionnaires, etc.
  - Audio/video equipment
  - Note-taking equipment

How to conduct usability (testing) studies?



System evaluation

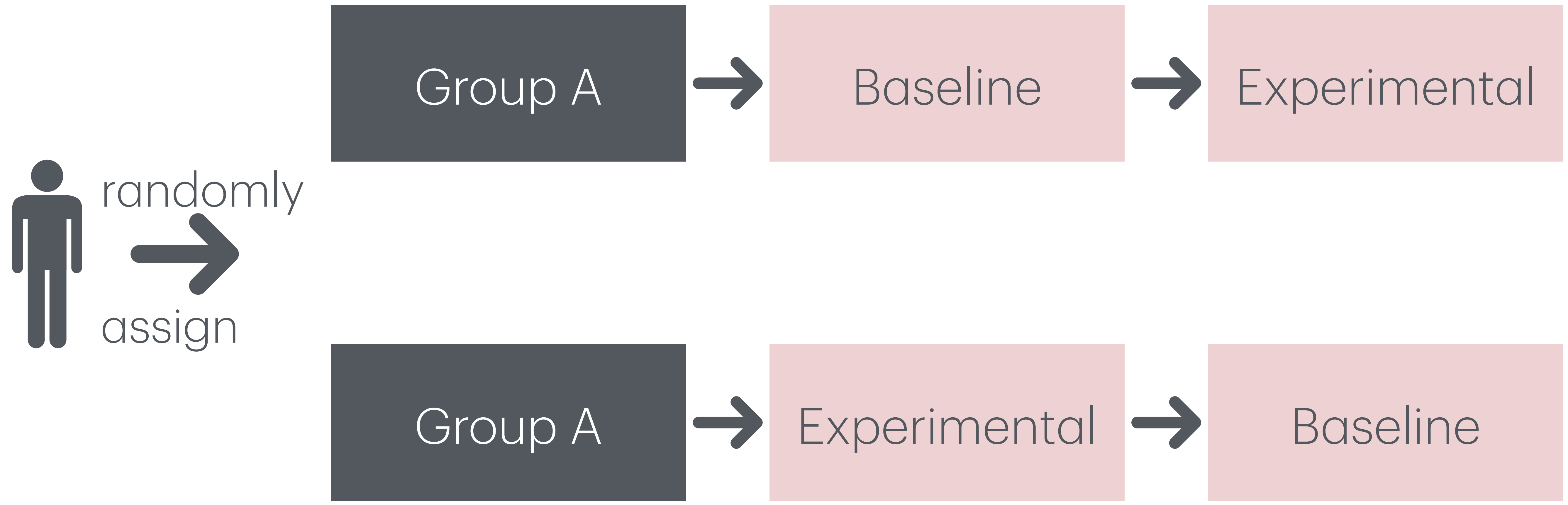
- Task-driven: Create tasks that represent common use cases for participants to complete
- Baseline vs. Experimental Conditions
  - Usually want to achieve statistically significant improvement in key performance metrics (e.g., time, task completion, accuracy, SUS, NASA/TLX)

Avoid confounding factors

Learning effect: In between-subjects studies, the tasks for the baseline and experimental condition are usually different to avoid learning effect

Treatment order: Counterbalanced study design

Hawthorne effect: Refer to the conditions as "system 1 and 2" rather than "baseline and experimental"



An example of counterbalanced design

Recap

- Types of projects suitable for this class: Systems (artifacts), Social sciences (empirical)
- Human-centered research methods
  - Qualitative
  - Quantitative
  - Interviews
  - Usability studies

Action items

- By the noon this Wednesday (Sept 18)
  - Submit this week's reading commentaries
  - Two students will lead the first discussion
- Project proposal due one week later (Sept 25 midnight)
  - **Book an office hour appointment with me (Wednesday 1-2pm)**