

Turning Privacy Risk Assessment into 20 Questions for Developers

Qiyu Li Haojian Jin



University of California San Diego

Articulating Privacy-related Design Decisions

Zoom Attendee Attention Tracking

The image shows a Zoom interface with two main panels. The left panel, titled "Participants (4)", lists four participants: Joshua Jones (Host, me), Aglae Cuevas, Nancy Williams, and Thomas Nguyen. A red box highlights a clock icon next to Aglae Cuevas, and a larger red box highlights a large clock icon. The right panel, titled "Meeting Participants", contains a table with columns: Name (Original Name), User Email, Leave Time, Duration (Minutes), and Attentiveness Score. A red box highlights the "Attentiveness Score" column header and a cell containing "100.0%". Another red box highlights the text "Attentiveness Score" and "100.0%" in a separate white box. A blue "Export" button is visible in the top right of the table panel.

Name (Original Name)	User Email	Leave Time	Duration (Minutes)	Attentiveness Score
Tom Leslie	toml@iup.edu	03/18/2020 09:09:34 AM	13	100.0%
Veronica Paz	vpaz@iup.edu	03/18/2020 08:59:48 AM	10	100.0%

I want to design an attendee attention tracking feature for a video conferencing app.



QUESTION 1

Would attention tracking be opt-in or opt-out for attendees?

Determines whether attendees must explicitly agree before being tracked.

Opt-in (attendee must consent)

Opt-out (enabled by default)

Always on (no choice)

[Write custom answer](#)

Confirm

PRIVACY DESIGN DECISIONS



Q1

Would attention tracking be opt-in or opt-out for attendees?

I want to design an attendee attention tracking feature for a video conferencing app.



QUESTION 2

When would attendees be notified about attention tracking?

Affects whether attendees are aware of tracking before, during, or after it happens.

Just-in-time (when joining)

At install time

Periodically during meeting

Never

[Write custom answer](#)

Confirm

PRIVACY DESIGN DECISIONS

Q1

Would attention tracking be opt-in or opt-out for attendees?

→ Always on (no choice)

Q2

When would attendees be notified about attention tracking?

I want to design an attendee attention tracking feature for a video conferencing app.



QUESTION 3

Would the host only see aggregated attention data?

Individual scores reveal each person's behavior; aggregated data only shows group trends.

Aggregated only

Individual scores

Both aggregated and individual

[Write custom answer](#)

Confirm

PRIVACY DESIGN DECISIONS

- Q1
Would attention tracking be opt-in or opt-out for attendees?
→ Always on (no choice)
- Q2
When would attendees be notified about attention tracking?
→ Just-in-time (when joining)
- Q3
Would the host only see aggregated attention data?

I want to design an attendee attention tracking feature for a video conferencing app.



QUESTION 4

Would this feature only be available in education settings?

Education contexts may have different norms around monitoring than corporate meetings.

Education only

Education and training

All meeting types

Configurable per org

[Write custom answer](#)

Confirm

PRIVACY DESIGN DECISIONS

- Q1
Would attention tracking be opt-in or opt-out for attendees?
→ Always on (no choice)
- Q2
When would attendees be notified about attention tracking?
→ Just-in-time (when joining)
- Q3
Would the host only see aggregated attention data?
→ Individual scores
- Q4
Would this feature only be available in education settings?

Key Privacy Design Decisions

1. Opt-in or opt-out?
 2. Show aggregated data only, or individual scores?
 3. When to notify – at install, just-in-time, or periodically?
 4. Restrict to education settings?
 5. Is the notification always on?
 6. How is attention inferred?
 7. Process data on-device, or in the cloud?
 8. What is the data retention period?
 9. Who can access the data?
 10. Let users report prediction errors?
-

Existing Privacy Threat Modeling Frameworks

PIA

Privacy Impact Assessment

System name Owner

Purpose: describe the data practice and operational need

- What personal information is collected?
- Who can access or share it?
- How long is it retained?

LINDDUN

Linkability

Identifiability

Non-repudiation

Detectability

Disclosure of information

Unawareness

Non-compliance

NIST PRAM

WS1 Business objectives

WS2 System design

WS3 Risk prioritization

WS4 Control selection

NIST Privacy Risk Assessment Methodology (PRAM)

ASSESS SYSTEM DESIGN

enumerate *data actions*

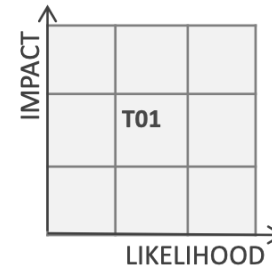
- Collection
- Generation
- Transformation
- Use
- Disclosure
- Retention
- Disposal

ANALYZE THREATS & HARMS

- Dignity Loss
- Discrimination
- Economic Loss
- Loss of Autonomy
- Loss of Liberty
- Loss of Trust
- Physical Harm

PRIORITIZE RISKS

Risk = Likelihood × Impact



- Share w/ 3rd party **821**
- Track location **659**
- Analyze behavior **577**
- Collect from social **379**

MITIGATION & CONTROLS

select controls

- Access Control
- De-identification
- Data Minimization
- Notice & Consent
- Encryption
- Retention Limits

Observational Study of NIST PRAM with Novice Developers

12 participants

students & junior software engineers

4 task scenarios

conducted real PRAM assessments after a brief training walkthrough

Think-aloud observation

how they worked through PRAM worksheets and what they found challenging

 Attention Tracking

 Smart Home Assistant

 Pregnancy Coupon

 Genetic Testing

Three Challenges in the PRAM Study

- 1 Overlooked privacy-related design opportunities
- 2 Limited awareness of alternative options
- 3 Hard to allocate attention across many decisions

PrivacyAkinator

Articulating Key Privacy Design Decisions using LLM-Generated Multiple-Choice Questions

① Input the design goal

Design an attendee attention tracking feature for a video conferencing application.

② Edit functional requirements

Data Collection

- Capture application window focus state from user's device
- Record timestamps when attention state changes

Data Processing & Storage

- Calculate the percentage of attention time for each individual
- Store processed attention metrics for 30 days

User Interface and Presentation

- Display a clock icon next to inattentive participants
- Provide hosts with meeting summary of each participant

③ Answer LLM-generated questions

Question 1 >>

Would users be notified before their attention status is collected during screen sharing?

Select an answer: [Write Custom Answer](#)

Yes

No

< Previous Skip Next >



④ Assess system design and privacy risks

Data Actions	Summary Issues	Potential Problems for Individuals	Likelihood	Impact	Risk
Collect application focus status	Lack of multitasking exceptions may create false readings of inattention	Discrimination Loss of Trust	7	17	119
	Limited opt-out mechanism (account settings only) may not provide sufficient control at the point of use	Loss of Autonomy	6	20	120
Process attention status	Processing method doesn't distinguish between legitimate and non-legitimate reasons for switching applications	Dignity Loss Loss of Trust	2	17	34
Store attention data	Individual-level granularity increases privacy risk compared to aggregate data	Dignity Loss Loss of Trust	6	32	192
	30-day retention may exceed necessary period for feature functionality	Loss of Trust Economic Loss	5	19	95
Notice of attention status	Persistent indicator may create anxiety or behavior modification	Dignity Loss Loss of Autonomy	2	15	30
	Limited transparency about what specific behaviors are being monitored	Loss of Trust Loss of Autonomy	6	25	150
Access attention report	Participants have limited control over who can access their attention data	Loss of Trust Loss of Autonomy	7	36	252
Process data deletion	Questions about verification of complete deletion	Loss of Trust Economic Loss	5	10	50

LINDDUN



Linkability



Identifiability



Non-repudation



Detectability



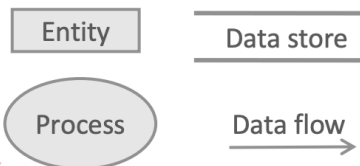
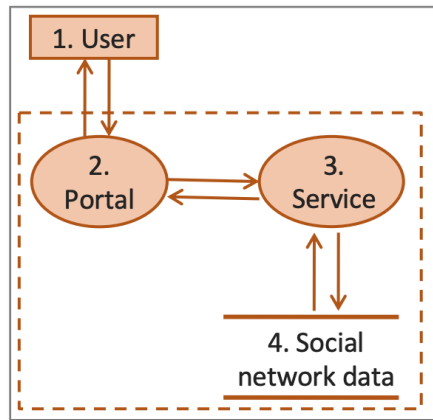
Disclosure of information



Unawareness



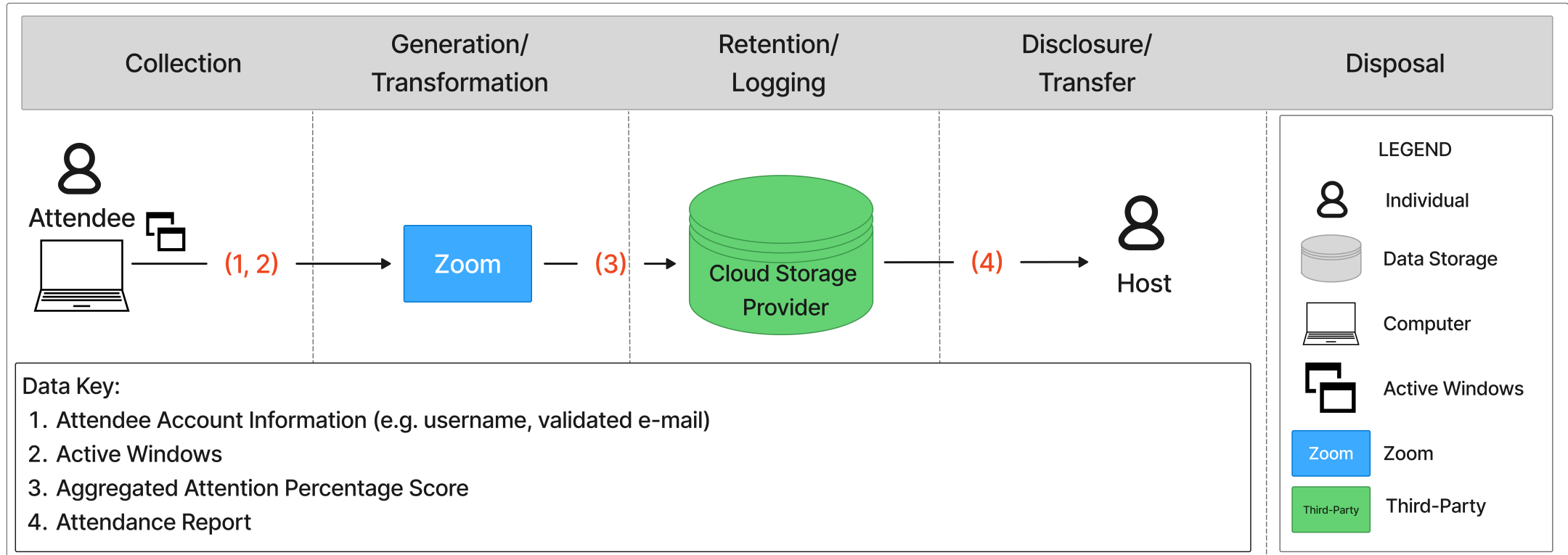
Non-Compliance



	Threat target	L	I	N	D	D	U	N
Data store	Social network db	X	X	x	x	X		X*
Data flow	User-portal data stream	X	X			X		X
						X

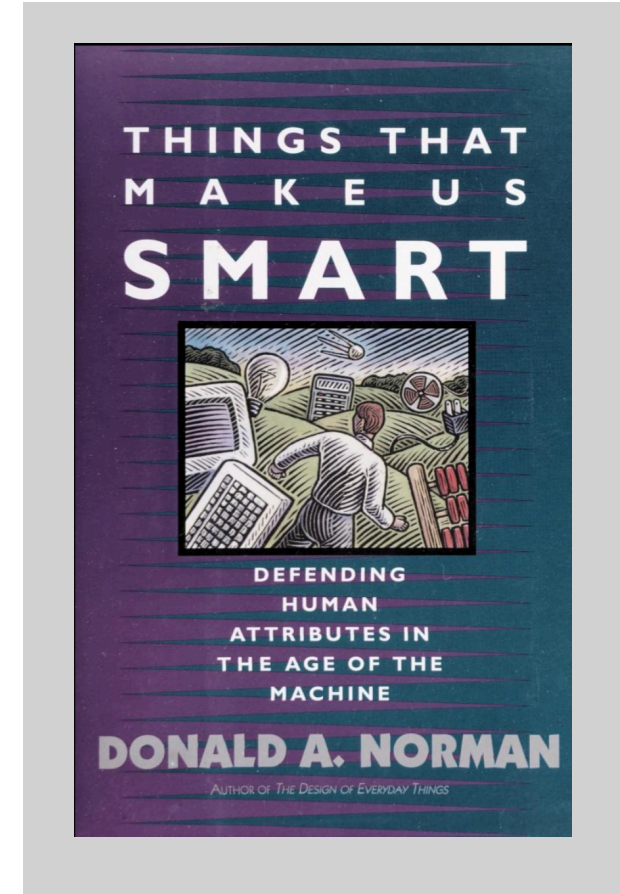
MAPPING TEMPLATE	LINDDUN	L	I	N	D	D	U	N
	PRIVACY THREAT MODELING							
Data store		X	X	X	X	X		X
Data flow		X	X	X	X	X		X
Process		X	X	X	X	X		X
Entity		X	X				X	

Data Flow Diagram (DFD)



"A good representation captures what matters for the task, and deliberately omits the rest."

– *Things That Make Us Smart*

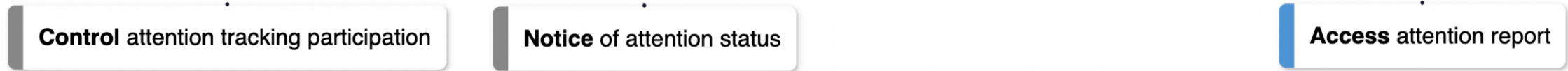


Verb-based Privacy Representation

Data flow



Stakeholder interactions



Design choices

Collect application focus status
DataType: Application focus status
Frequency: Continuously
Timing: During screen sharing in meetings
Method: Client application monitoring

Method

Data-Driven Privacy Design Space

TECHCRUNCH

Zoom tracked whether attendees paid attention to screen shares

Zoom's attention-tracking feature monitored whether the app was the **active window** on participants' screens. The feature was **enabled by default** with **no notification** to attendees. Hosts received a **per-person attention score** in a post-meeting report.

10K privacy news articles



```
COLLECT data_type
app_focus_status Whether Zoom is the active window

COLLECT frequency
continuous Monitored throughout entire meeting

CONSENT consent_mode
opt-out Enabled by default, user must disable

NOTIFY notification
none No notice shown to attendees

SHARE aggregation
individual Host sees per-person scores

SHARE recipient
meeting_host Report delivered to host only
```

Extract design decisions



```
Collect
data_type
app_focus_status · GPS · audio
frequency
continuous · one-time · periodic

Consent
consent_mode
opt-in · opt-out · implicit

Notify
notification
just-in-time · install · none

Share
aggregation
individual · aggregated
recipient
meeting_host · third_party
```

Iterative open coding

Results

Data-Driven Privacy Taxonomy

Domain Labels: **Health** **Social Media** **Demographic** **Financial** **Personality** **Social / personal Network** **Location** **Credential** **Behavior** **Preferences** **Data Actions** **Stakeholder Interactions**

Collect	Process	Share	Notify
<ul style="list-style-type: none"> Universal Keys with Global Values Location <ul style="list-style-type: none"> On the edge Cloud servers Hybrid Frequency <ul style="list-style-type: none"> One month Forever Never Method <ul style="list-style-type: none"> Through client app Server algorithm Universal Keys with Domain-specific Values <ul style="list-style-type: none"> Data Type <ul style="list-style-type: none"> Browsing behavior (Behavior) Profile information (Personality) Demographic information (Demograph) Transaction data (Financial) 	<ul style="list-style-type: none"> Universal Keys with Global Values <ul style="list-style-type: none"> Location Universal Keys with Domain-specific Values <ul style="list-style-type: none"> Inputdata Method <ul style="list-style-type: none"> Algorithmic filtering (Social Media) Data analysis software (Social Media) User flagging system (Social Media) Domain-specific Keys and Values <ul style="list-style-type: none"> Pregnancy prediction (Health) <ul style="list-style-type: none"> Identify pregnancy patterns Medical diagnosis Detect distress signals Identify sensitive signals 	<ul style="list-style-type: none"> Universal Keys with Global Values <ul style="list-style-type: none"> Method <ul style="list-style-type: none"> In-app advertisement Email Mail to Physical Address Universal Keys with Domain-specific Values <ul style="list-style-type: none"> Target <ul style="list-style-type: none"> Account User (Social Network) Recommended users (Social Network) Data Type <ul style="list-style-type: none"> App pop-up advertisement (Credential) In app notification (Credential) Coupon (Credential) 	<ul style="list-style-type: none"> Universal Keys with Global Values <ul style="list-style-type: none"> Recipient Item Analysis <ul style="list-style-type: none"> In-app Email Purchasing screen in physical store Universal Keys with Domain-specific Values <ul style="list-style-type: none"> Analysis Timing <ul style="list-style-type: none"> Before item purchased (Behavior) In-app account created (Behavior)
	<h3>Consent</h3> <ul style="list-style-type: none"> Universal Keys with Global Values <ul style="list-style-type: none"> Opt-in options <ul style="list-style-type: none"> Implicitly Explicitly 	<h3>Control</h3> <ul style="list-style-type: none"> Domain-specific Keys and Values <ul style="list-style-type: none"> Promotion Reference (Behavior) <ul style="list-style-type: none"> Preference setting No control for user 	<h3>Request</h3> <ul style="list-style-type: none"> Domain-specific Keys and Values <ul style="list-style-type: none"> Sensitive Data Deletion (Preferences) <ul style="list-style-type: none"> Purchasing data User profiles Browsing history Checklist history

Exploratory question

Question 1

Would users be notified before their attention status is collected during screen sharing?

SELECT AN ANSWER

[Write custom answer](#)

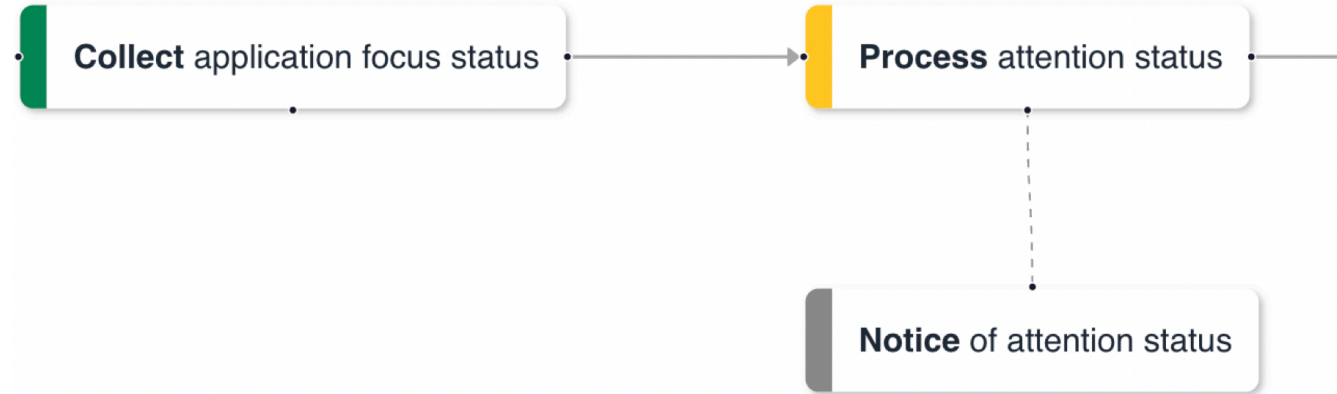
Yes

No

[< Previous](#)

[Skip](#)

[Next >](#)



Exploratory question

Question 1

Would users be notified before their attention status is collected during screen sharing?

SELECT AN ANSWER

[Write custom answer](#)

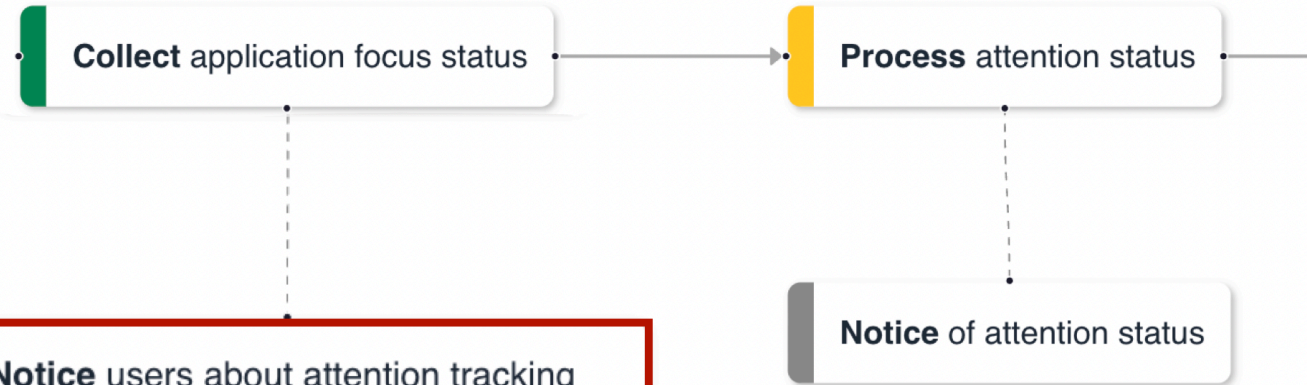
Yes

No

< Previous

Skip

Next >



Notice users about attention tracking before collection

+ **Content:** Information about attention tracking during screen sharing

+ **Form:** Pre-meeting notification

+ **Recipient:** Meeting participants

Exploitative question

Question 6

The system stores attention status and percentage data after processing

How long would attention data be retained after processing?

SELECT AN ANSWER

[Write custom answer](#)

During the active meeting

24 hours after meeting ends

7 days after meeting ends

30 days after meeting ends

Until manually deleted by admin

< Previous

Skip

Next >

Process attention percentage

Store attention data

Access attention report

Exploitative question

Question 6

The system stores attention status and percentage data after processing

How long would attention data be retained after processing?

SELECT AN ANSWER

[Write custom answer](#)

During the active meeting

24 hours after meeting ends

7 days after meeting ends

30 days after meeting ends

Until manually deleted by admin

< Previous

Skip

Next >

Process attention percentage

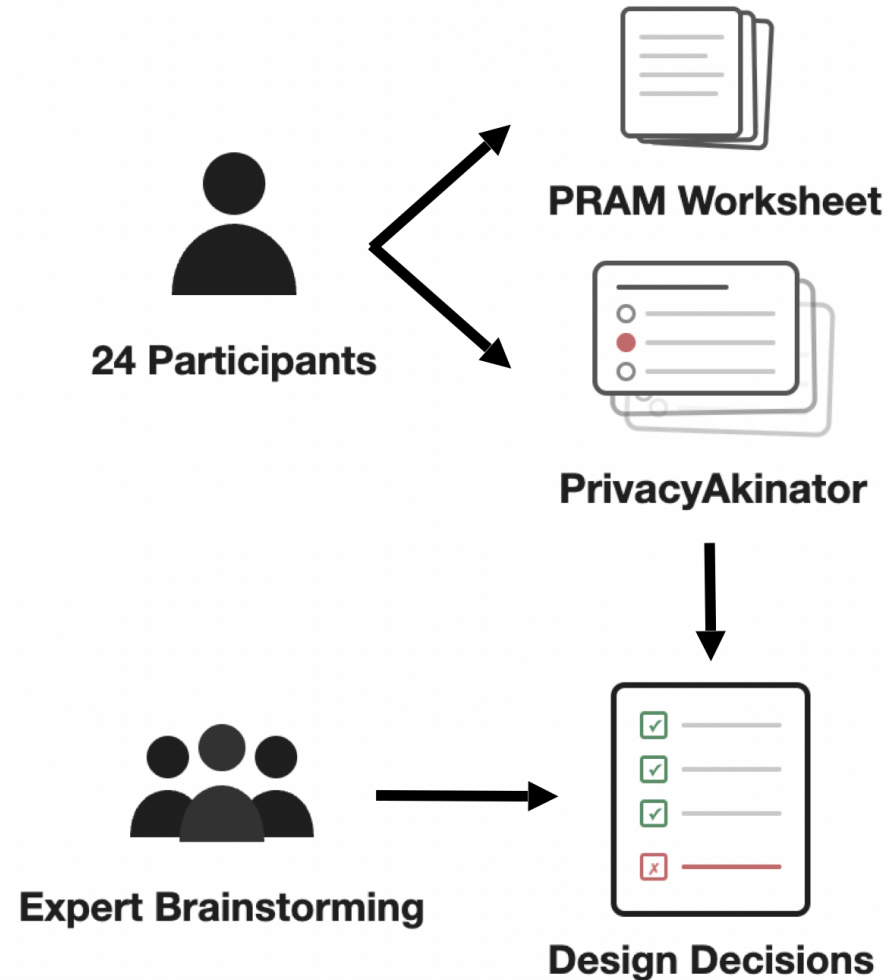
Store attention data

+ RetentionPeriod: 30 days

Access attention report

Method

User Study



24 students & junior developers

Identify privacy-related design decisions

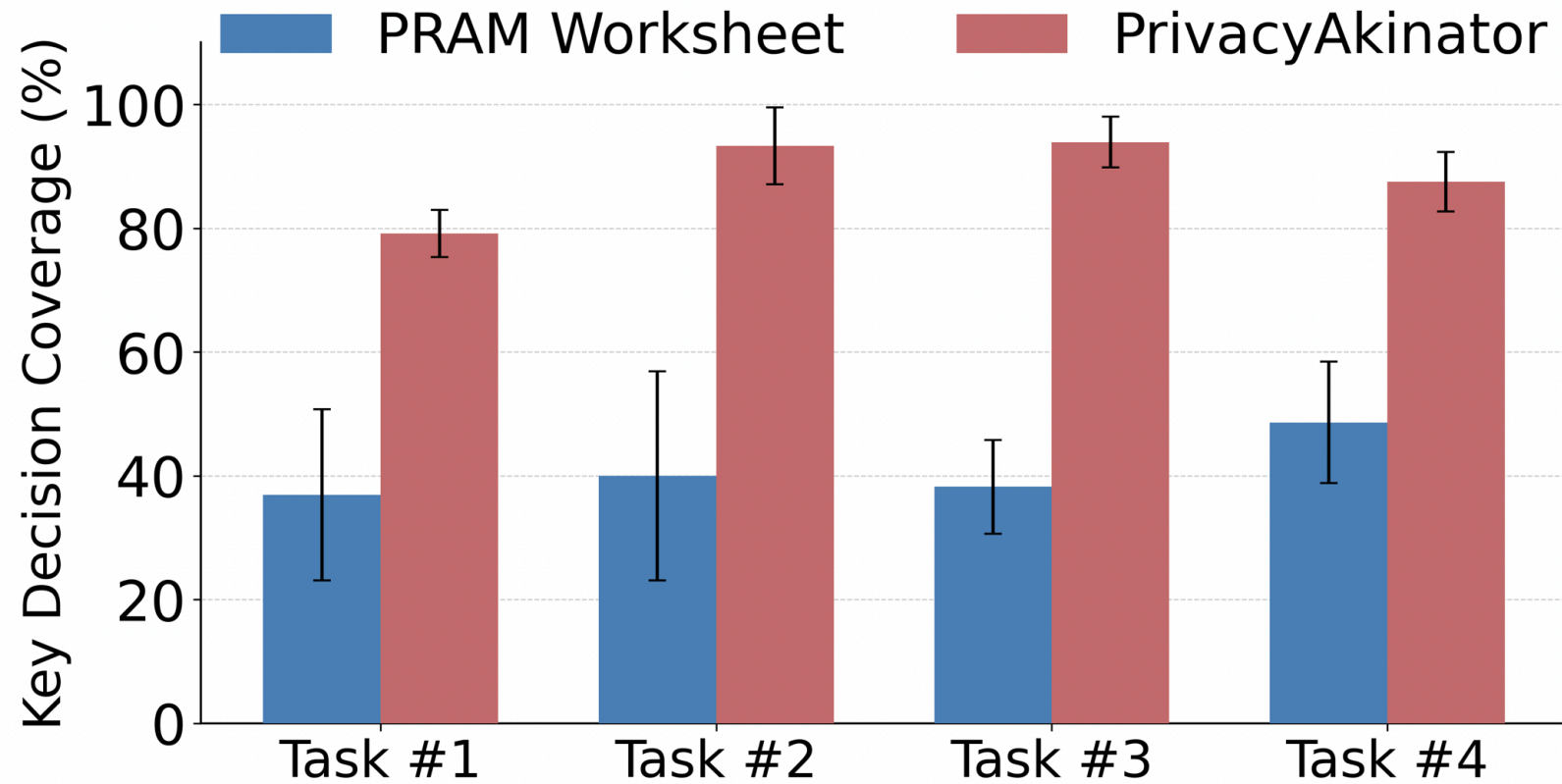
Conditions: PRAM worksheets vs. our tool

Ground Truth: Expert brainstorming

Findings

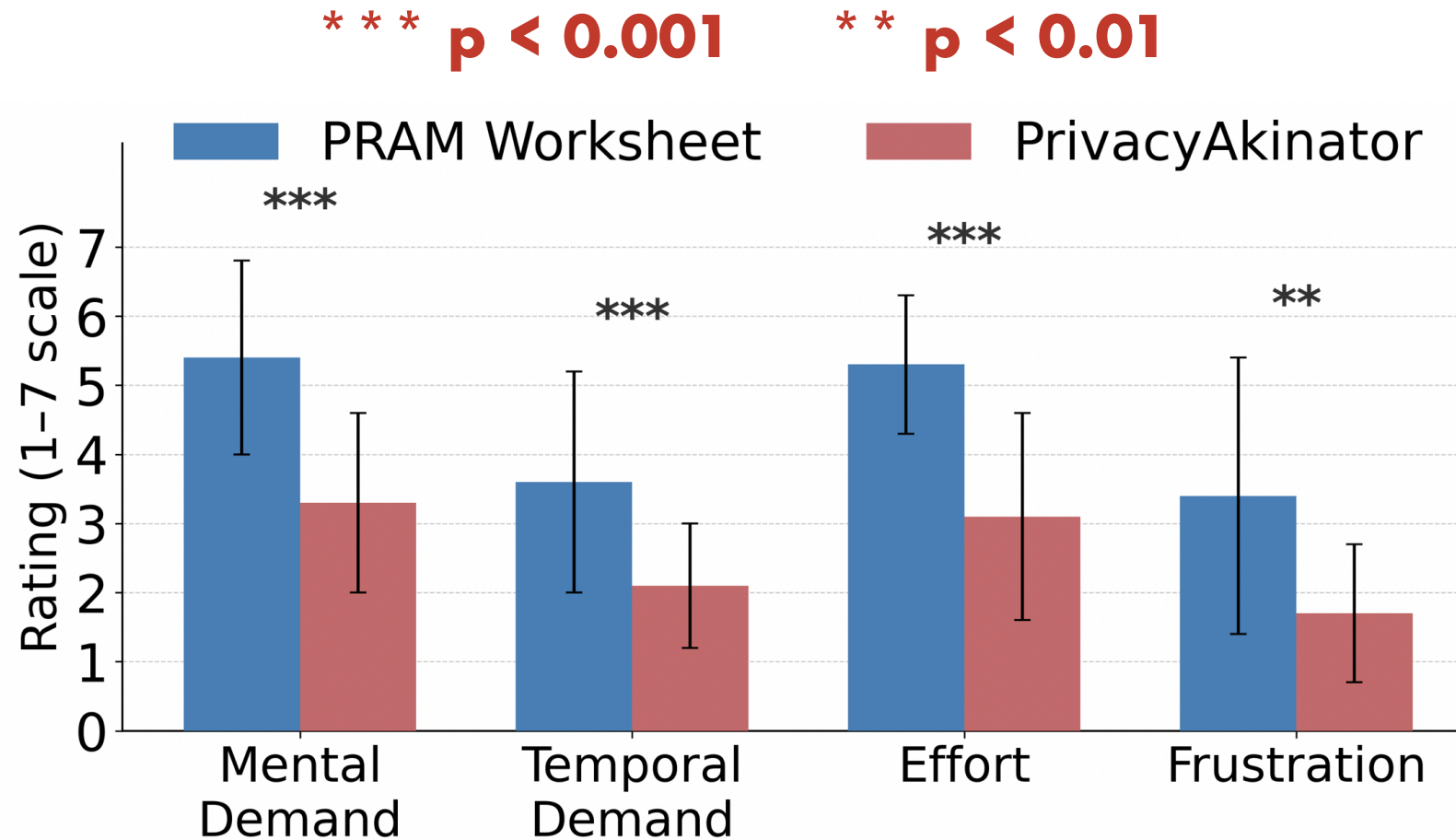
Helps developers identify more privacy-related design decisions

Coverage: **89% vs. 42%**



Findings

Also significantly reduces cognitive load



Next Steps

ASSESS SYSTEM DESIGN

enumerate *data actions*

Collection

Generation

Transformation

Use

Disclosure

Retention

Disposal

ANALYZE THREATS & HARMS

Dignity Loss

Discrimination

Economic Loss

Loss of Autonomy

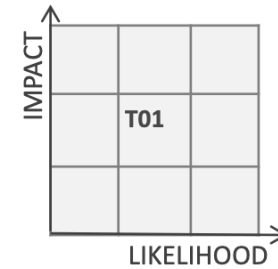
Loss of Liberty

Loss of Trust

Physical Harm

PRIORITIZE RISKS

Risk = Likelihood × Impact



Share w/ 3rd party **821**

Track location **659**

Analyze behavior **577**

Collect from social **379**

MITIGATION & CONTROLS

select controls

Access Control

De-identification

Data Minimization

Notice & Consent

Encryption

Retention Limits

ONGOING WORK

Turning Privacy Risk Assessment into 20 Questions

I want to design an attendee attention tracking feature for a video conferencing app.



QUESTION 4

Would this feature only be available in education settings?

Education contexts may have different norms around monitoring than corporate meetings.

Education only

Education and training

All meeting types

Configurable per org

[Write custom answer](#)

Confirm

PRIVACY DESIGN DECISIONS

- Q1
Would attention tracking be opt-in or opt-out for attendees?
→ Always on (no choice)
- Q2
When would attendees be notified about attention tracking?
→ Just-in-time (when joining)
- Q3
Would the host only see aggregated attention data?
→ Individual scores
- Q4
Would this feature only be available in education settings?

Qiyu Li
qiyuli@ucsd.edu