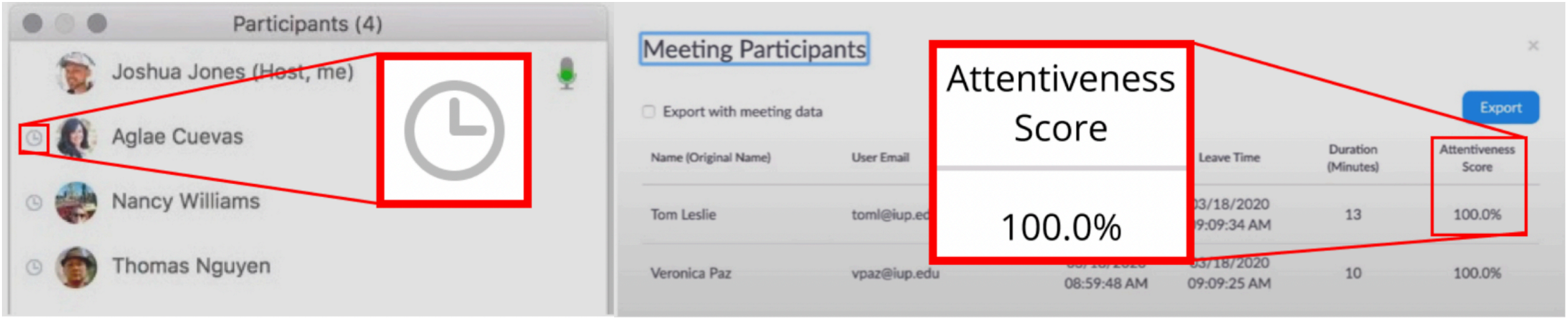
Turning Privacy Risk Assessment into 20 Questions for Developers

Qiyu Li Haojian Jin

University of California San Diego

Articulating Privacy-related Design Decisions

Zoom Attendee Attention Tracking



[1] Li, T. W. et al. Redesigning Privacy with User Feedback: The Case of Zoom Attendee Attention Tracking. *ACM CHI 2024*.

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

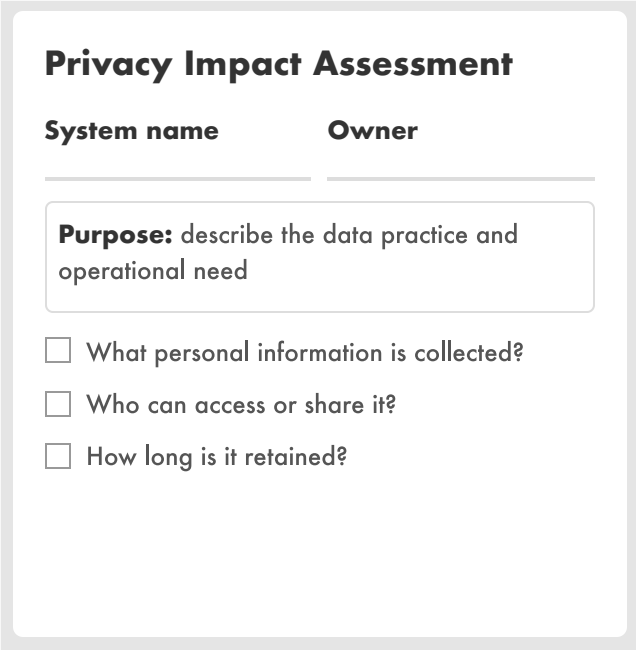
1. Opt-in or opt-out?
2. Show aggregated data only, or individual scores?
3. When to notify – at install, just-in-time, or periodically?
4. Restrict to education settings?
5. Is the notification always on?
6. How is attention inferred?
7. Process data on-device, or in the cloud?
8. What is the data retention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

.....

[1] Li, T. W. et al. Redesigning Privacy with User Feedback: The Case of Zoom Attendee Attention Tracking. *ACM CHI 2024*.

Existing Privacy Threat Modeling Frameworks

PIA



LINDDUN

- **L**inkability
- **I**dentifiability
- **N**on-repudiation
- **D**etectability
- **D**isclosure of information
- **U**nawareness
- **N**on-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*

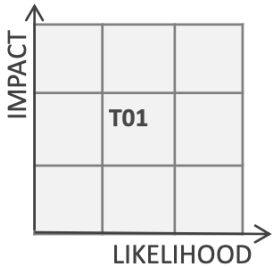
- Collection
- Generation
- Transformation
- Use
- Disclosure
- Retention
- Disposal

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

[2] NIST. "NIST privacy framework: a tool for improving privacy through enterprise risk management." NIST CSWP 01162020, 2020.

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

zoom Attention Tracking

alexa Smart Home Assistant

target Pregnancy Coupon

23andMe 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

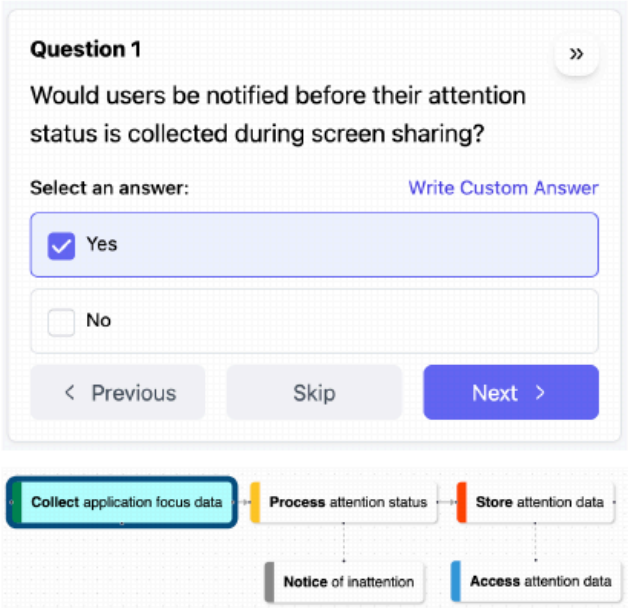
Data Processing & Storage

- 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



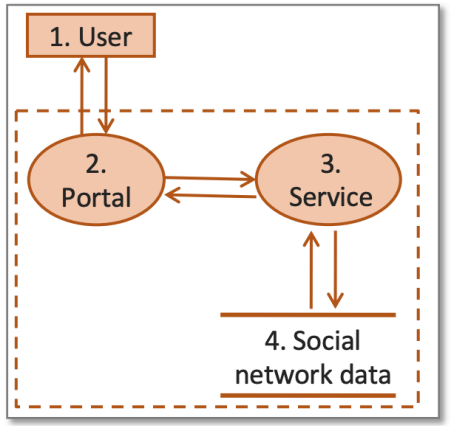
④ Assess system design and privacy risks

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

[3] Li, Q. et al. PrivacyAkinator: Articulating Key Privacy Design Decisions using LLM-Generated Multiple-Choice Questions. *ACM CHI 2026.*

LINDDUN

- Linkability
- Identifiability
- Non-repudation
- Detectability
- Disclosure of information
- Unawareness
- Non-Compliance



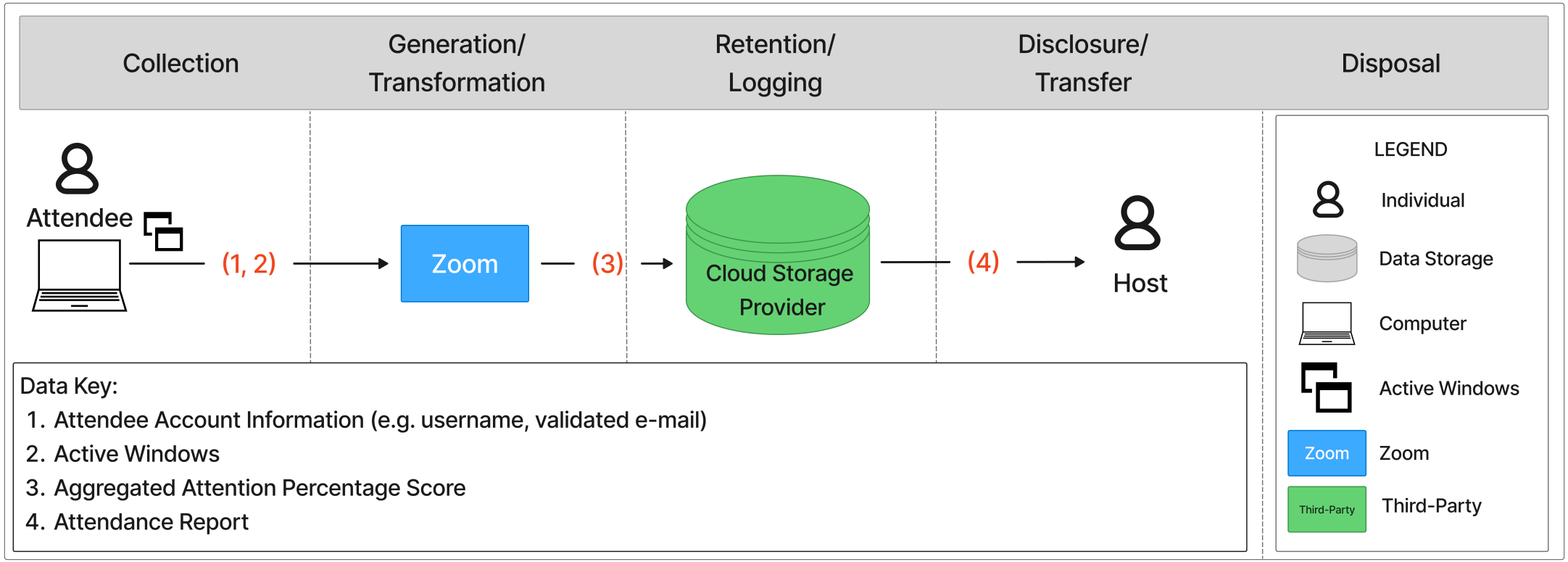
	Threat target	L	I	N	D	D	U	N
Data store	Social network db	X	X	x	x	X		X*
Data flow	User-portal data stream	X	X			X		X
	...	...						X

MAPPING TEMPLATE

LINDDUN	L	I	N	D	D	U	N
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	

[4] Deng, M. et al. "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements." *Requirements Engineering* 16(1), 2011.

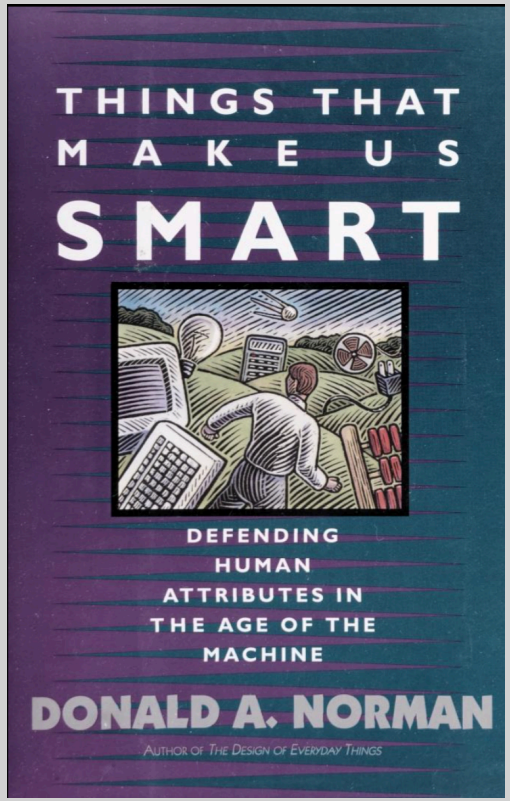
Data Flow Diagram (DFD)



[5] Li, Q. and Chen, Y. "Data Flow Diagram." Springer Berlin Heidelberg, 2009.

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

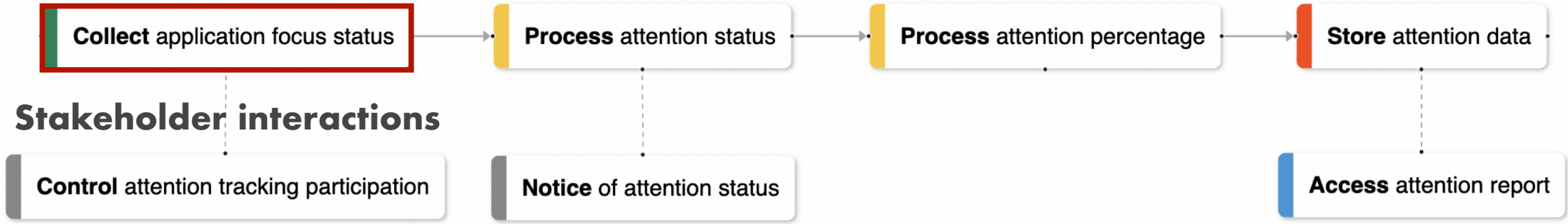
— *Things That Make Us Smart*



[6] Norman, D. A. Things That Make Us Smart. Addison-Wesley, 1993.

Verb-based Privacy Representation

Data flow



Design choices

Collect application focus status

DataType: Application focus status

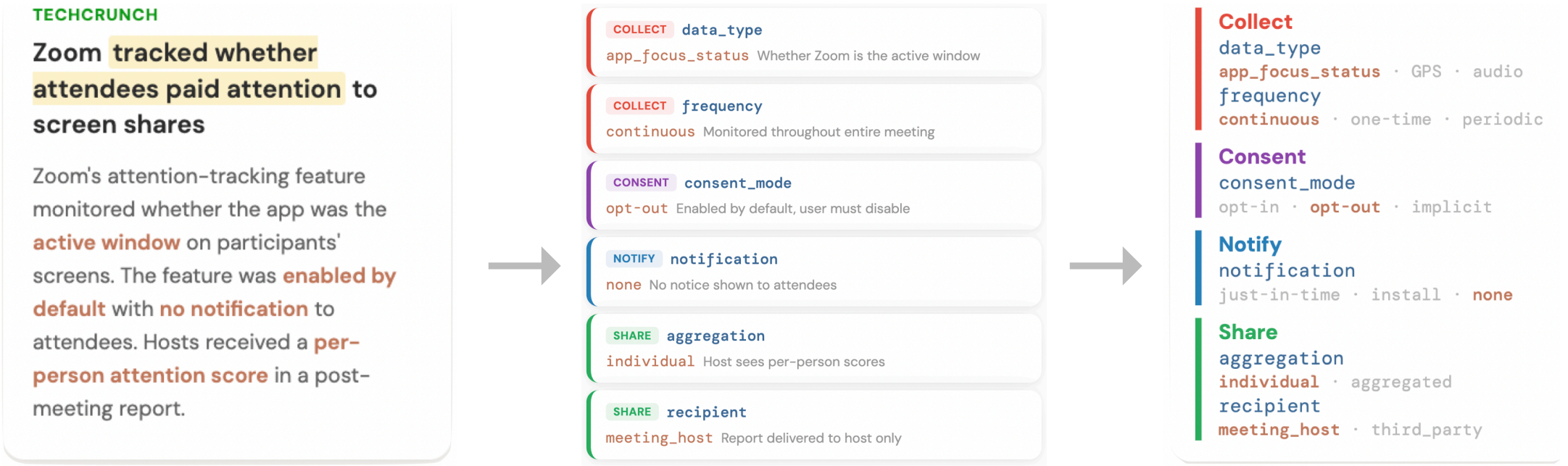
Frequency: Continuously

Timing: During screen sharing in meetings

Method: Client application monitoring

Method

Data-Driven Privacy Design Space

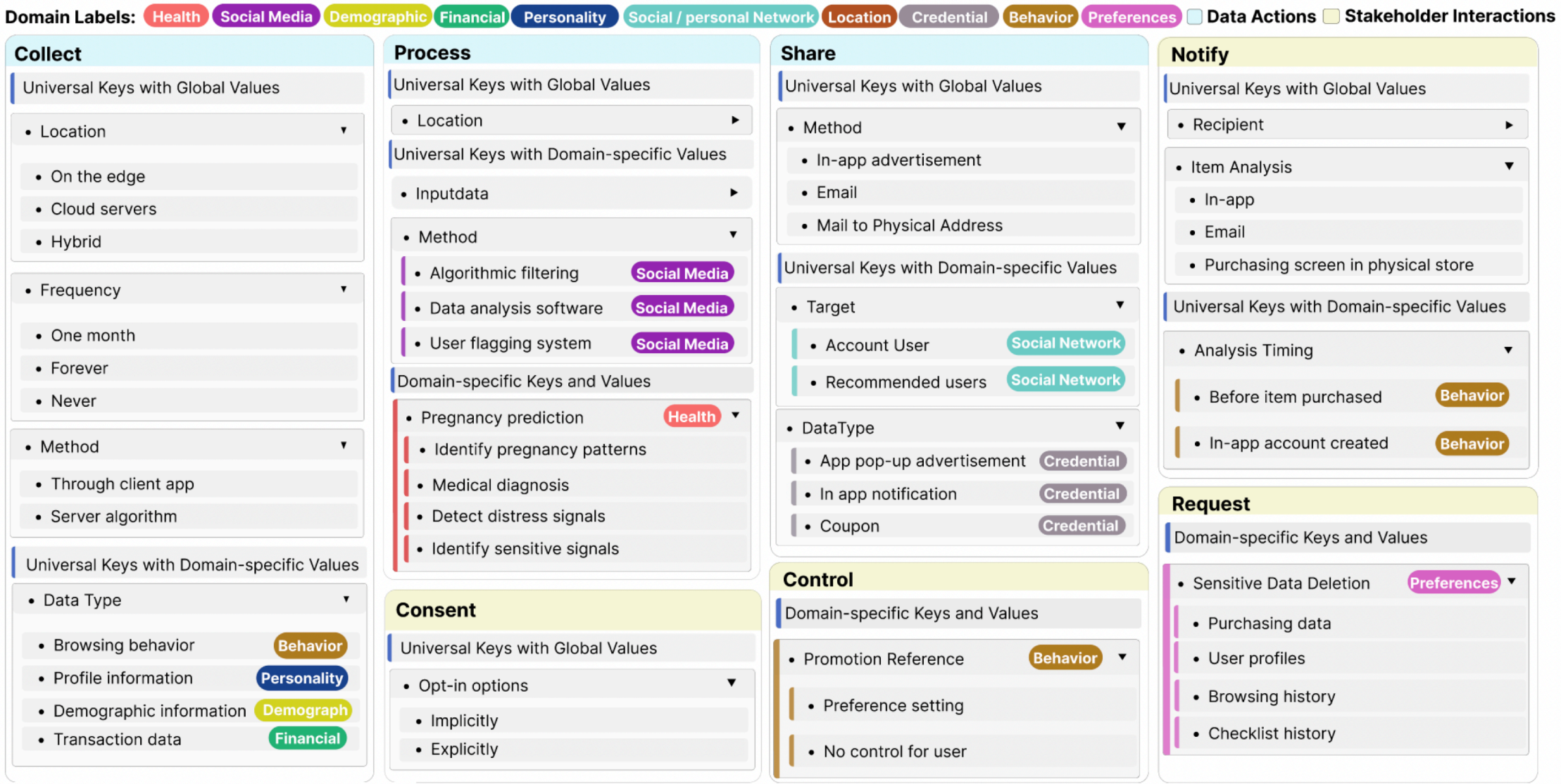


10K privacy news articles

Extract design decisions

Iterative open coding

Data-Driven Privacy Taxonomy



Exploratory question

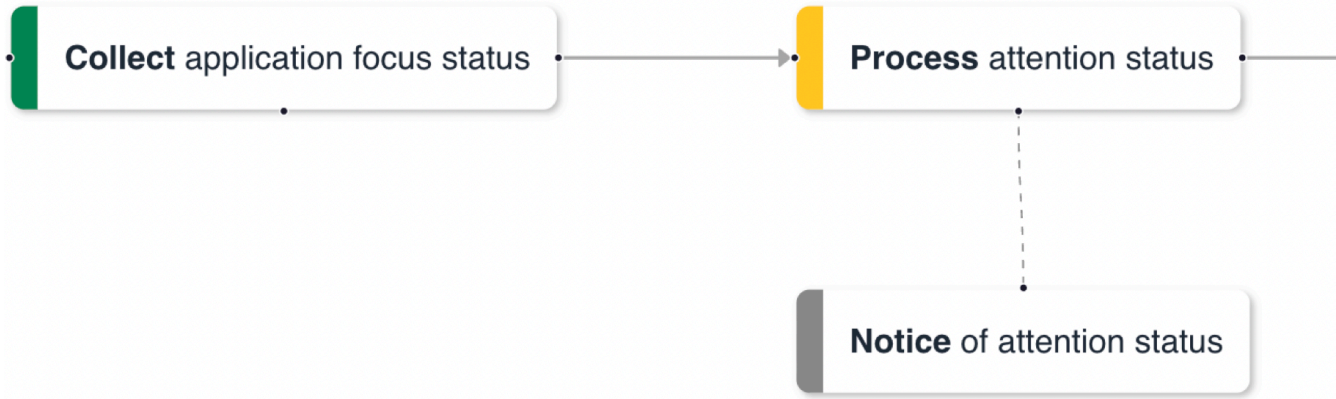
Question 1

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

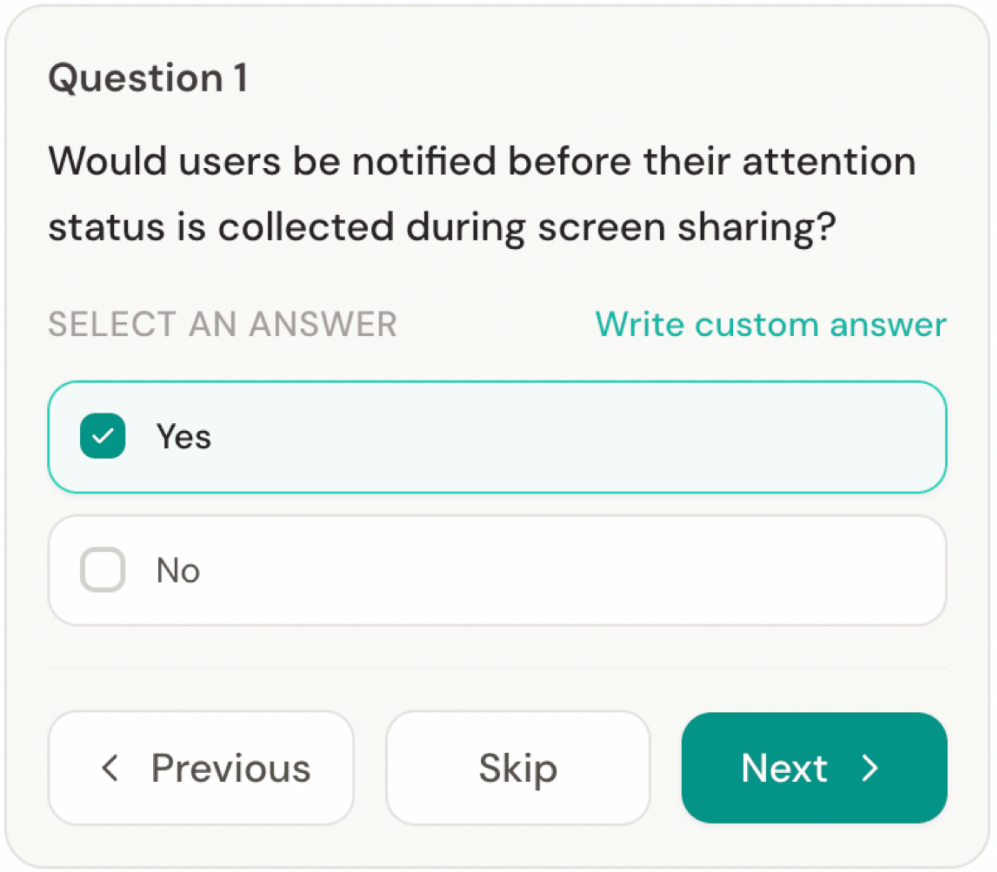
SELECT AN ANSWER Write custom answer

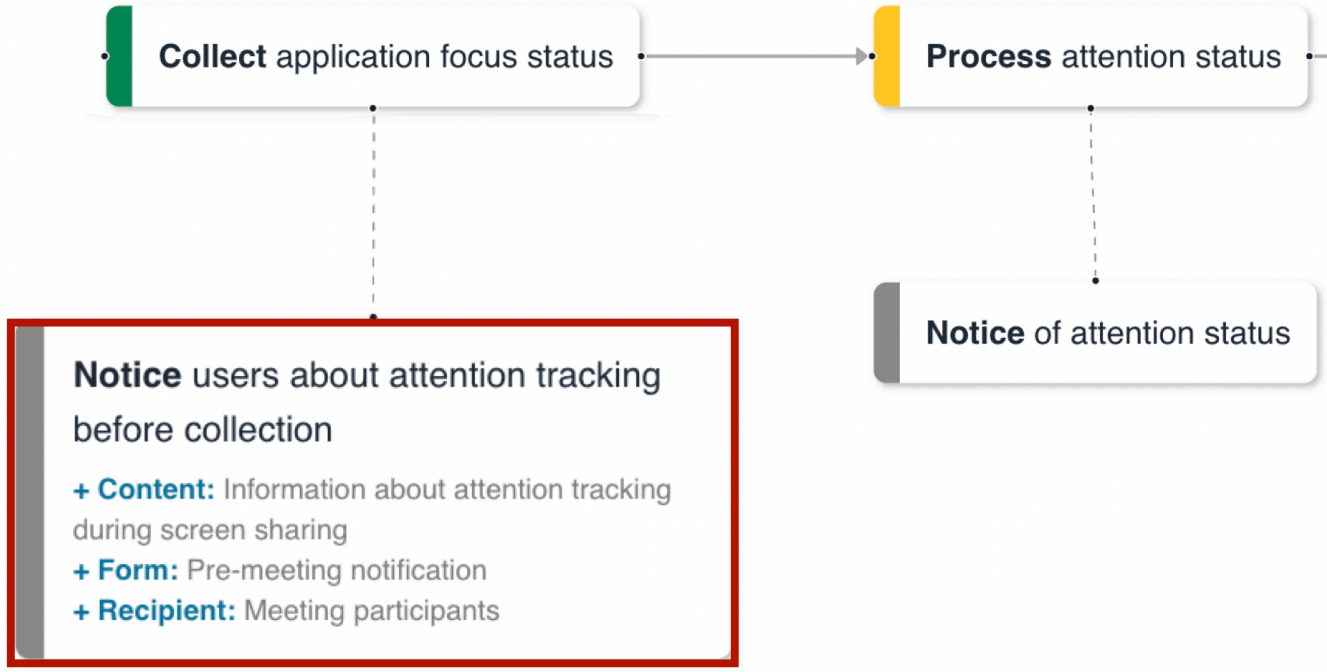
- [x] Yes
- [ ] No

< Previous Skip Next >



Exploratory question





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
- [x] 30 days after meeting ends
- [ ] Until manually deleted by admin

< Previous Skip Next >

Exploitative question

Question 6

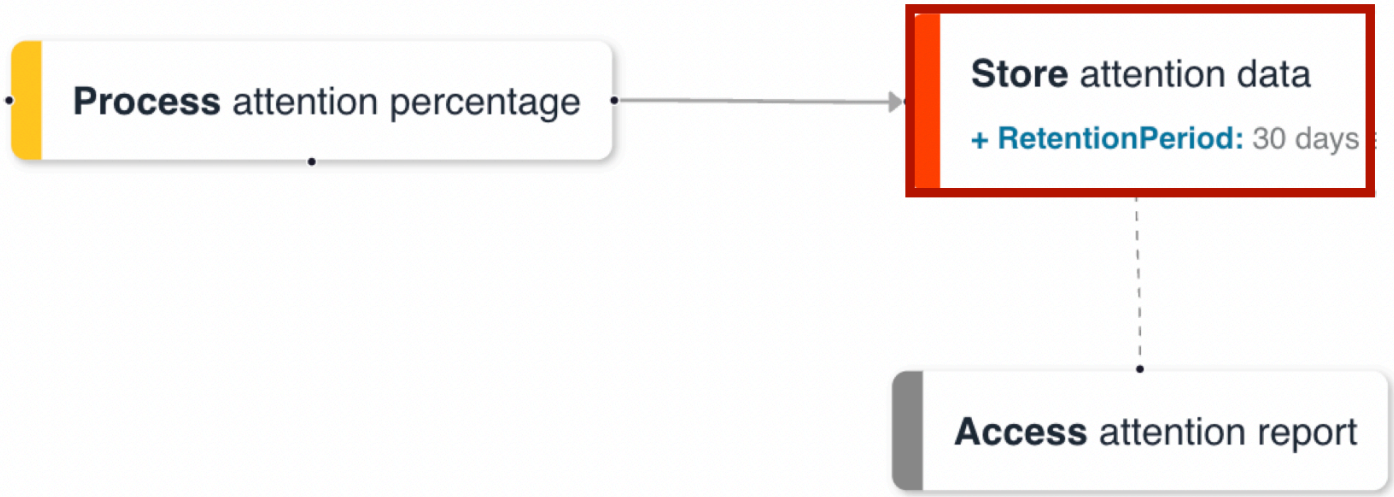
The system stores attention status and percentage data after processing

How long would attention data be retained after processing?

SELECT AN ANSWER Write custom answer

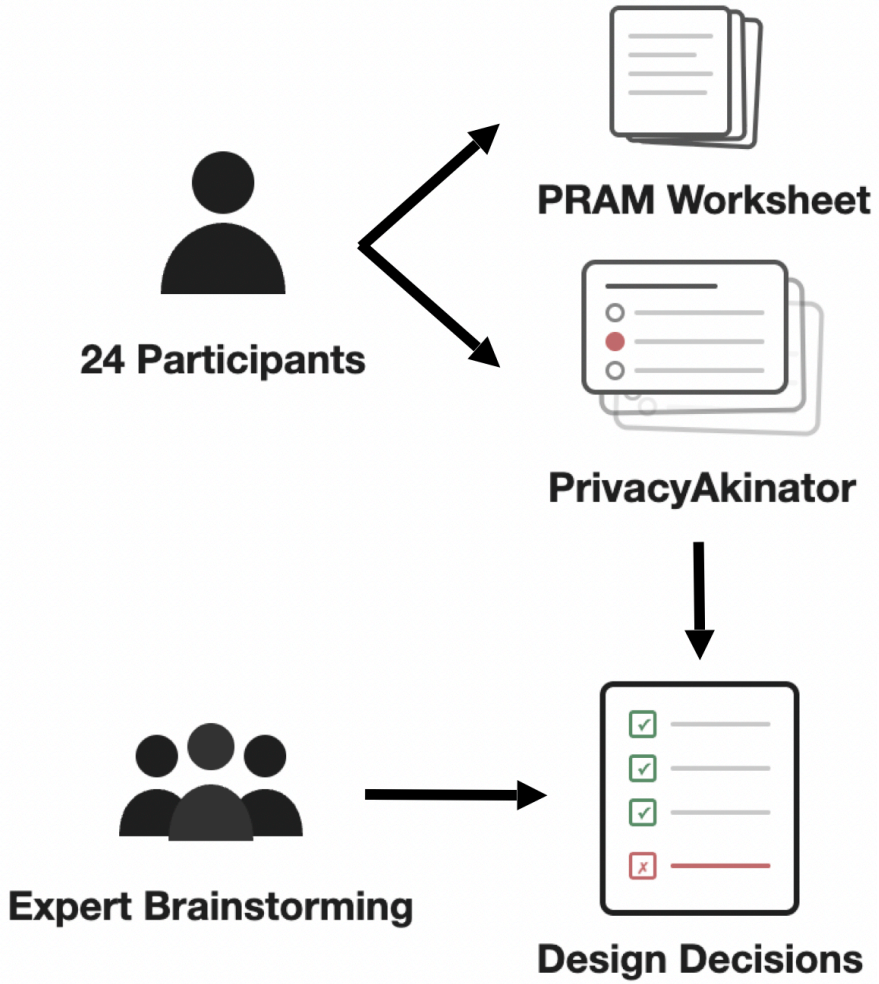
- [ ] During the active meeting
- [ ] 24 hours after meeting ends
- [ ] 7 days after meeting ends
- [x] 30 days after meeting ends
- [ ] Until manually deleted by admin

< Previous Skip Next >



Method

User Study



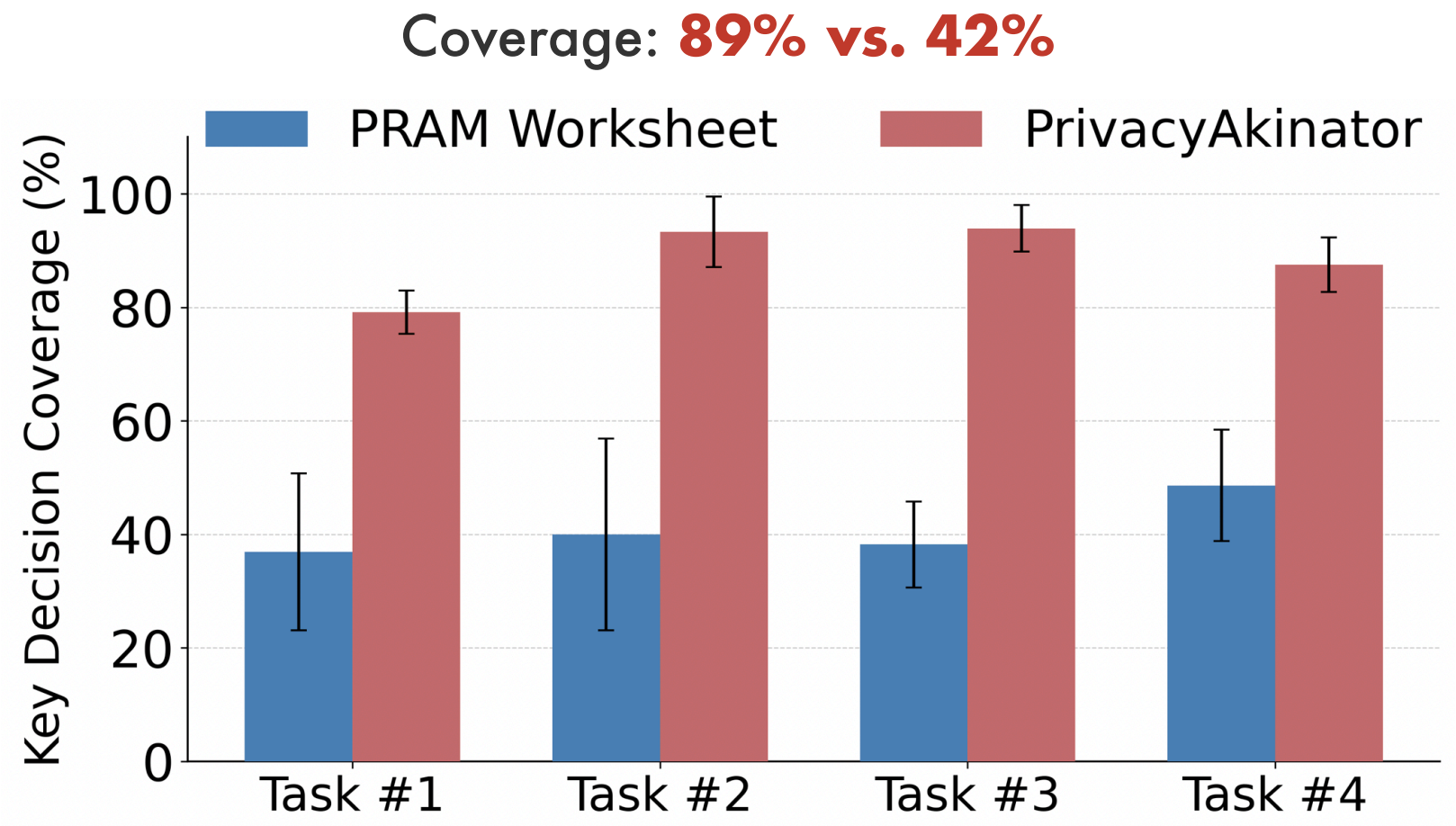
24 students & junior developers

Identify privacy-related design decisions

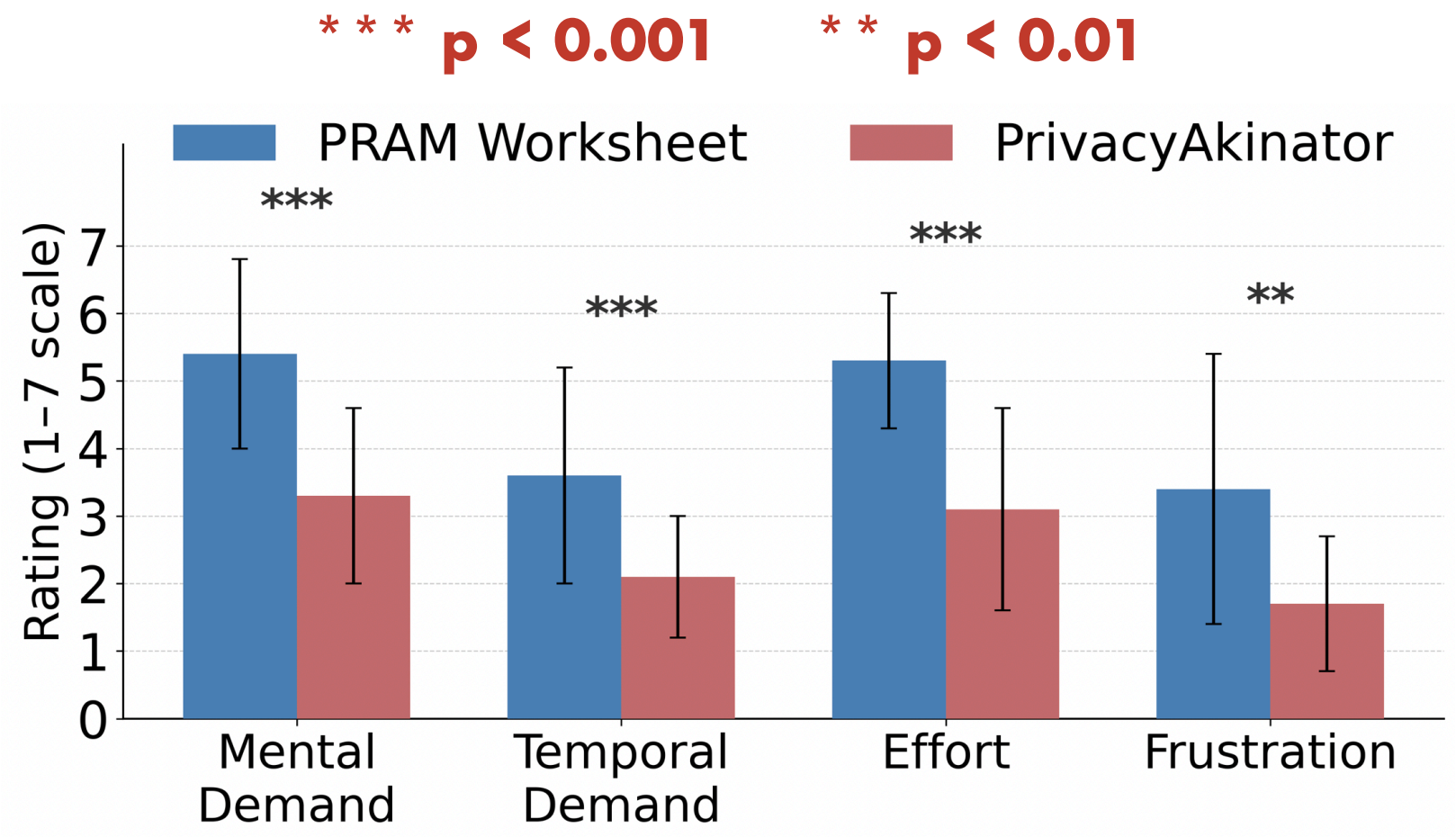
Conditions: PRAM worksheets vs. our tool

Ground Truth: Expert brainstorming

Helps developers identify more privacy-related design decisions



Also significantly reduces cognitive load



Next Steps

ASSESS SYSTEM DESIGN

enumerate *data actions*

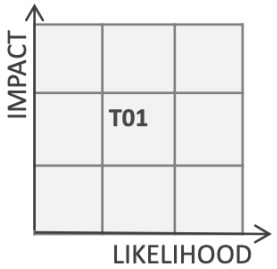
- Collection
- Generation
- Transformation
- Use
- Disclosure
- Retention
- Disposal

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

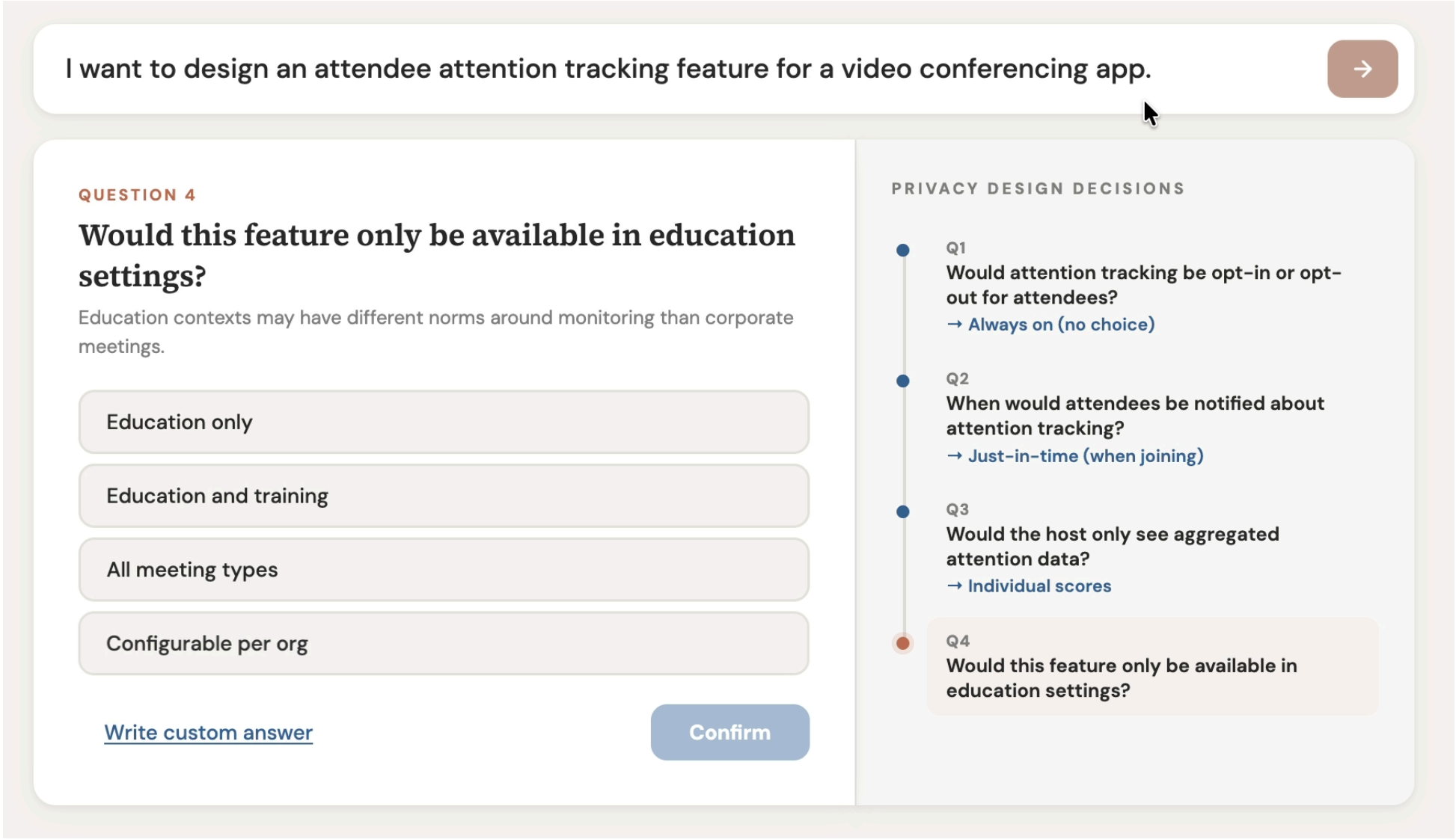
MITIGATION & CONTROLS

select *controls*

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

ONGOING WORK

Turning Privacy Risk Assessment into 20 Questions



Qiyu Li
qiyuli@ucsd.edu