Vision: Human-as-the-Unit Privacy Management with *AI Agents*

PEACH Lab
Privacy-Enabling AI &
Computer-Human Interaction Lab

Northeastern University

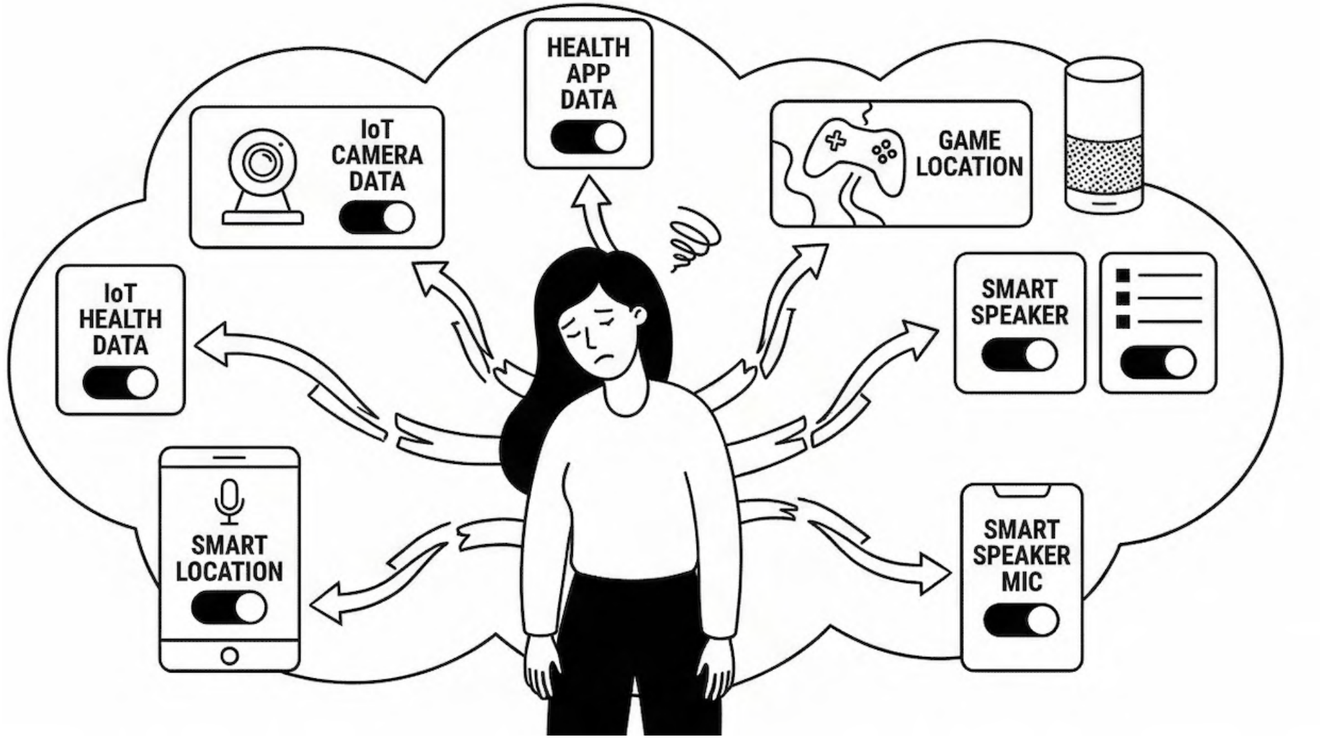
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Eryue Xu

Tianshi Li

How can AI help with our privacy?

Think through privacy management challenges as *a user*…



Current privacy control:

- Domain- or application-specific

In Reality:

- Tasks are done via multiple apps
- Privacy fatigue + data overload

AI Agents (Automation + Intelligence) **for**

Human-as-the-Unit Privacy Management

- **First, we interviewed 12 participants to learn their cross-context privacy concerns.**

We heard ***rich*** cross-context privacy challenges.

Cross-application challenges

“Let’s say someone(on the dating app) wants to find me, they Google my name(on the dating app) and Strava account pops up on Google (with my full name and locations)." (P12)

We heard ***rich*** cross-context privacy challenges.

Cross-temporal challenges

“I really didn’t have any internet safety skills... I signed up when I was 13. I used to post more personal information. Now I don’t really post... I’ve made some of my posts unavailable to the public.” (P5)

We heard ***rich*** cross-context privacy challenges.

Cross-interpersonal challenges

“I have to respect my friend’s privacy. Maybe they don’t want me to post it to the wild.” (P6)

We heard *rich* cross-context privacy challenges.

Cross-app
- Information flow transparency
- Inadequate privacy risk assessment
- Identification protection challenges
- Misaligned expectations with carious platform privacy design

Cross-time
- Digital footprint management overload
- Evolving privacy preferences
- Accumulated data management deficiencies

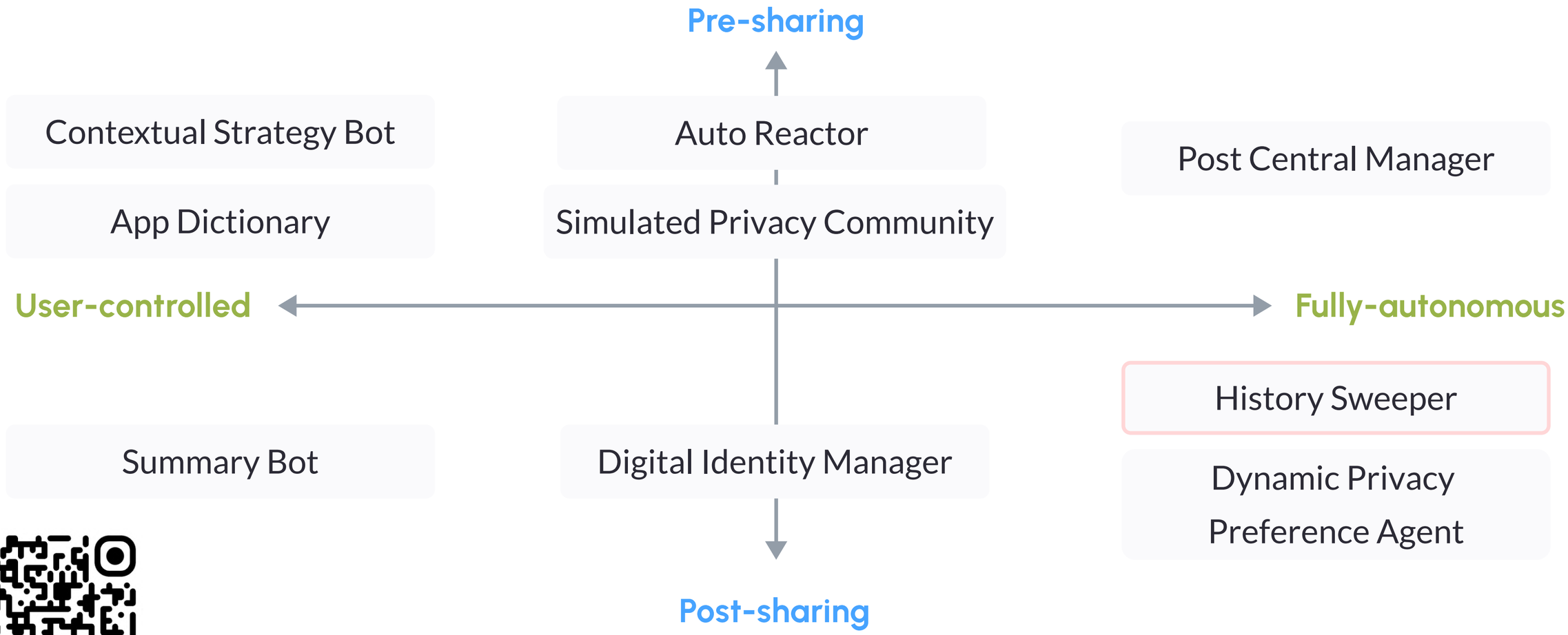
Cross-person
- Interpersonal privacy boundary complications
- Granular relationship-based sharing challenges

FULL Paper

- First, we interviewed 12 participants to learn their cross-context privacy concerns.
- Next, we brainstormed 9 AI-agent-for-privacy ideas and have 116 participants evaluated them via a speed dating survey.

FULL Paper

Our Ideations



FULL Paper

User evaluation

We found that people like *post-sharing* and *automated* solutions.

Rank	Design Idea	Timing	User Agency	Relatability	Effectiveness
1	*Digital Identity Manager*	Post	Half-autonomous	5	4
2	*Dynamic Privacy Preference Agent*	Post	Fully-autonomous	5	4
3	*History Sweeper*	Post	Fully-autonomous	5	4
4	*Post Central Manager*	Pre	Fully-autonomous	5	4
5	*Summary Bot*	Post	User-controlled	4	3
6	*Contextual Strategy Bot*	Pre	User-controlled	4	3
7	*App Dictionary*	Pre	User-controlled	5	4
8	*Auto Redactor*	Pre	Half-autonomous	4	4
9	*Simulated Privacy Community*	Pre	Half-autonomous	4	4

We used Plackett-Luce method to calculate the worth of each idea and ranked them globally.

What does this mean for privacy AI agent?

Post-sharing **data management opportunities are in the interpersonal context!**

Institutional post-sharing data management is in a black box.

Interpersonal post-sharing data management can be achieved at GUI level.

What does this mean for privacy AI agent?

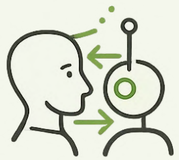
Users show good confidence in AI’s capability, which is a good sign of positive adoptions of these technologies.

What does this mean for privacy AI agent?

Implementing AI Agents for Cross-context Privacy

Loss of awareness

Single point of failure



Adjustable autonomy
+ lightweight confirmation from users

Bounded permission
+ minimized collecting data

Robustness against adversarial outcomes

Vision: Human-as-the-Unit Privacy Management with *AI Agents*

Eryue Xu

eryuexu2@illinois.edu

My LinkedIn

FULL Paper