Zhiping (Arya) Zhang

Email: zhang.zhip@northeastern.edu Website: zhipingzhang.com Google Scholar

My PhD research lies at the intersection of **HCI**, **privacy** and **human-centered AI**.
Specifically, I 1) understand privacy challenges in personalized agentic AI systems; and 2) design effective human-AI collaboration mechanisms that align AI behavior with both general social norms and individual privacy preferences in real-world applications.

Education

Ph.D. student in Computer Science — Boston, US
Northeastern University (NEU), Supervisor: Prof. Tianshi Li — 2024 – 2029 (Exp.)

M.Sc. in Industrial Design (HCI Track) — Eindhoven, NL
Eindhoven University of Technology (TU/e) — 2018 – 2020

B.Eng. in Industrial Design (Honours, Top 1) — China & UK
University of Liverpool (UoL), Xi'an Jiaotong-Liverpool University — 2014 – 2018

Research Experience

Privacy-Enabling AI & Computer-Human Interaction Lab — 2024 – present
Conducted human-centered privacy research on language models and agentic AI systems using mixed methods, system building, and computational experiments. First-authored papers published in CHI '24 [C.2], CSCW '25 [C.3], and submitted to TOCHI [I.1].
(Advised by *Prof. Tianshi Li*)

CompLING Lab-AI Group, UWaterloo — Summer 2025
Led a project on mitigating privacy concerns in personalized LM agents by balancing human control and agent autonomy. Developed an LLM agent system and conducted a computational experiment. First-authored paper submitted to COLM '26 [I.2].
(Advised by *Prof. Freda Shi*)

Social Robotics Lab, TU/e — 2019
Worked on social robot role design, robot behavior programming, and conducted a field test. Co-authored paper published in HRI '20 [C.1].
(Advised by *Prof. Emilia Barakova & Panos Markopoulos*)

Industry Experience (full-time)

AI Product Manager, *Fiture* — 2021 – 2023
0-to-1 explored AI-powered home gym equipment, bridging algorithms and real products (*a voice assistant, natural language & body-pose remote control, and a course searching and recommendation system*).

User Experience Design & Research, *Alibaba* — 2020 – 2021
Researched and designed user experience to support multi-role collaboration in enterprise purchasing systems. (*an intelligent purchasing conversational agent*: enhanced purchasers' workflow and increased user satisfaction by 22% after launch).

* indicates co-first authorship.

Peer-reviewed conference and journal papers

[C.4] **Dark Patterns Meet GUI Agents: LLM Agent Susceptibility to Manipulative Interfaces and the Role of Human Oversight**
Jingyu Tang*, Chaoran Chen*, Jiawen Li, Zhiping Zhang, Bingcan Guo, Ibrahim Khalilov, Simret Araya Gebreegziabher, Bingsheng Yao, Dakuo Wang, Yanfang Ye, Tianshi Li, Ziang Xiao, Yaxing Yao, Toby Jia-Jun Li
In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '26)

[C.3] **Secret Use of Large Language Model (LLM)**
Zhiping Zhang, Chenxinran Shen, Bingsheng Yao, Dakuo Wang, Tianshi Li.
In Proceedings of the ACM on Human-Computer Interaction (CSCW '25)

[C.2] **"It's a Fair Game", or Is It? Examining How Users Navigate Disclosure Risks and Benefits When Using LLM-Based Conversational Agents**
Zhiping Zhang, Michelle Jia, Hao-Ping (Hank) Lee, Bingsheng Yao, Sauvik Das, Ada Lerner, Dakuo Wang, Tianshi Li.
In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)

[C.1] **Robot role design for implementing social facilitation theory in musical instruments practicing**
Heqiu Song, Zhiping Zhang, Emilia I. Barakova, Jaap Ham, Panos Markopoulos
In Proceedings of the 2020 ACM/IEEE International Conference on Human-Robot Interaction (HRI '20).

In Submission

[I.2] **Autonomy Matters: A Study on Personalization-Privacy Dilemma in LLM Agents**
Zhiping Zhang, Yi Evie Zhang, Freda Shi, Tianshi Li

[I.1] **Privacy Leakage Overshadowed by Views of AI: A Study on Human Oversight of Privacy in Language Model Agent**
Zhiping Zhang, Bingcan Guo, Tianshi Li

SIG/Poster/ Workshop

[W.1] **Toward a Human-centered Evaluation Framework for Trustworthy LLM-Powered GUI Agents**
Chaoran Chen*, Zhiping Zhang*, Ibrahim Khalilov, Bingcan Guo, Simret A Gebreegziabher, Yanfang Ye, Ziang Xiao, Yaxing Yao, Tianshi Li, Toby Jia-Jun Li
(HEAL @CHI '25)

[P.1] **The Obvious Invisible Threat: LLM-Powered GUI Agents' Vulnerability to Fine-Print Injections**
Chaoran Chen, Zhiping Zhang, Bingcan Guo, Shang Ma, Ibrahim Khalilov, Simret A Gebreegziabher, Ziang Xiao, Yaxing Yao, Tianshi Li, Toby Jia-Jun Li
(SOUPS '25)

[S.1] **Human-Centered Privacy Research in the Age of Large Language Models**
Tianshi Li, Sauvik Das, Hao-Ping (Hank) Lee, Dakuo Wang, Bingsheng Yao, Zhiping Zhang
In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)

Professional Service

Program Committee

2026: (Associate Chair) CHI '26 Poster, BiAlign @CHI '26, IUI '26, AgentCraft @IUI '26
2025: HAIPS @CCS '25

External Reviewer

❀ *Received "special recognitions" for outstanding reviews*
2026: ❀CHI '26, IMWUT '26, HRI '26, DIS '26
2025: ❀CHI '25, ❀UIST '25, IMWUT '25, TEI '25, IJHCS
2024: CSCW '24, CUI '24

Awards

IF Design Award Winner	2024
Reddot Award Winner	2023
IF Talent Award Winner	2020
Alibaba High-level Talents Scholarship (~$14,400)	2020
China-U.S Young Maker Competition Final Excellence Award	2018
Best Overall Academic Performance (Top 1)	2018
Academic Achievement Award Scholarship (Top 5%) (~$1,440)	2018
Academic Excellence Award Scholarship (Top 10%) (~$720)	2017
COMAP's Interdisciplinary Contest in Modeling - Meritorious Winner (Top 5%)	2016

Talks/Press

Autonomy Matters: A Study on Personalization-Privacy Dilemma in LLM Agents
ABSURD (Annual Boston Security Usability Research Day) Feb 2026

Dark patterns have long manipulated human behavior online. Now AI agents are falling for them, too
Northeastern Khoury News Jan 2026

"It's a Fair Game", or Is It? Examining How Users Navigate Disclosure Risks and Benefits When Using LLM-Based Conversational Agents
CHI May 2024